الجامعَة اللبنانيّة

كليّة الحقوق والعلوم السياسيّة والإداريّة

القوّة في الفضاءِ السيبراني: فصلٌ عصريٌّ من التحدّي والاستجابة

رسالة لنيل دبلوم دراسات عليا في العلوم السياسية والإدارية

إعداد

أنديرا عراجي

لجنة المناقشة

الدكتور محمود جبور	الأستاذ المشرف	رئيساً
الدكتور بلال عبدالله	أستاذ	عضواً
الدكتور كميل حبيب	أستاذ	عضواً

٢٠١٥-٢٠١٦

الجامعة اللبنانية غير مسؤولة عن الآراء الواردة في هذه الرسالة وهي تعبّر عن رأي صاحبها فقط.

شكر وإهداء

أتقدّم بجزيل الشكر للدكتور محمود جبور المحترم, والذي لم يكن أستاذا أكاديميا عاديّا, بل المشرف الدقيق, حيث اهتمّ بتفاصيل ومضامين الرسالة, فأثراها بتدقيقه اللغوي, وتصويب محتواها العلميّ. وكان الأب السند, والمحفّز, والداعم لي, لا سيّما عندما أرى صعوبة في الاستمرار, ولم يشكّك يوماً في قدرتي على إنجاز هذه الرسالة. فله مني كاملُ الشكر وبالغُ الامتنان, وأطلب الى الله أن يطيل بعمره.

كما أشكر عميد كلية الحقوق والعلوم السياسية والإدارية في الجامعة اللبنانية, الدكتور كميل حبيب المحترم, والذي شرّفني بقبوله أن يكون قارئا ثانٍ للرسالة. وأثمّن غالياً ملاحظاته, كذلك مساعدته في انجاز الترتيبات الإدارية المطلوبة.

كما يطيب لي أن أشكر القارئ الأول, الدكتور بلال عبدالله, وأدعو له بالتوفيق التام كمدير لمركز المعلوماتية القانونية, في الجامعة اللبنانية.

وأهدي عملي المتواضع هذا الى روح والدي محمد علي عراجي, رحمه الله, والى والدتي الغالية, التي أكنّ لها كلّ المحبة والشكر والامتنان, آدامها الله بكامل عافيتها. كما أهديه الى زوجي محمد عثمان, الذي كان المشجّع لي في الارتقاء الدائم. والى أولادي: الدكتور بسام عثمان, وعيسى عثمان, وفرح عثمان, الذين آمنوا بي.

المقدّمــة

كان لظهور الفضاء السيبراني, في أوائل الثمانينيات, أثرٌ بالغ في الحياة البشرية, وبأوجهها كافة, اذا صحّ التعبير. ومردّ ذلك بشكل أساسي, الى طبيعته الفريدة, هذا عدا عن الفرص التي قدمها, والتحديات التي طرحها. ففيه يمكن التجوّل, وبحريّة فائقة, وذلك بمجرد الضغط على مفتاح التشغيل, الخاص بالكمبيوتر, وحيث يتميّز استخدامه بالسهولة, ورخص التكلفة, والسرعة في الحصول على المعلومات, الموجودة بوفرة, هذا فضلا عن إمكانية مستخدمه التخفّي, وعدم الظهور بشخصيته الحقيقية. وقد أدّى ذلك, الى تعدّد العاملين فيه, بحيث طاول الدول والجماعات والأفراد والشركات, على حد سواء, كما تنوّعت استخداماته, لتشمل الشؤون التجارية, والمالية, والاقتصادية, والعسكرية, والاجتماعية.

واذا كان من الصعب, أحيانا كثيرة, تحريك أسطول دولة معينة, في المحيط أو الاقليم البحري, للقيام بمهام محددة, فإنّه من اليسير جدا, إرسال جيش جرار من الفيروسات, وبرامج الكمبيوتر, للقيام بعمليات سيبرانية, على قدر عال من الأهمية, ودرجة بالغة من الخطورة. وعليه, بدا الفضاء السيبراني, وبأحد أوجهه, ساحة جديدة للصراع , حيث يمكن تبادل الهجمات, وتنفيذ الأعمال العدوانية بين الخصوم, أسوة بباقي المجالات : كالبحر والبر والفضاء..

وتطرح من هذه الزاوية, مسألة الأمن فيه, بأبعاده كافة, لا سيما مع التوسع في الأخذ بما يسمى "الحكومة الإلكترونية", واتساع نطاق مستخدمي وسائل الاتصال وتكنولوجيا المعلومات في العالم, بحيث تصبح قواعد المعلومات القومية, في حالة انكشاف, أمام الخارج والداخل, على السواء. هذا فضلا عن المخاطر المتأتية عن المحتوى غير القانوني, لجهة التسويق للأفكار المتطرّفة, والترويج للإباحية, والقيام بأعمال تجسّس.

ويعتبر الصراع في الفضاء السيبراني, أحد أوجه الصراع الدولي, حيث تتوافر الاحتمالات الأشد خطورة, والأكثر تدميرا, مع الملاحظة, أن الأسلحة المستعملة, هي جدّ بسيطة, بحيث لا تتعدّى الكيلوبايت الواحد, هذا عدا عن أنها تعمل بسرية تامة, وكفاءة عالية, ومن دون تمييز بين المدنيين والمحاربين, أو بين العام والخاص.

وتتنوّع وسائل ممارسة القوة في العلاقات الدولية, تبعا لإمكانيات الدول. فقد تكون عسكرية, مالية, اقتصادية... وذلك للتغلّب على الخصم أو شلّ قدرته, وإضاعفه. لكنّ الفضاء السيبراني, أوجد معادلات جديدة. فالقّوة باتت موزّعة, ولم تعد محصورة بالدولة وحدها,الأمر الذي طرح على بساط البحث عددا من الاشكالات, تتمثل في الأسئلة التالية:

ما هي طبيعة هذه القوة؟ ومن يملكها فعلا؟ ما هي حدود التصرّف بها؟ وهل من ضوابط ؟ ما هي المجالات التي توظّف فيها؟ هل أنّ سباق التسلّح في هذا المجال, ينطوي على مخاطر شبيهة بتلك المترتّبة على استعمال الأسلحة التقليدية وغيرها؟ هل أنّ القوانين والمعاهدات الدولية القائمة صالحة للتطبيق في هذا الفضاء, أم أنّ هناك حاجة ماسة, لايجاد تشريعات جديدة مع طبيعته الخاصة؟

لقد دار النقاش, وما يزال , حسب طبيعة القوّة في المجال السيبراني, أهي قوّة صلبة, أم ناعمة, أم ذكية, من دون أن يتم التوصّل الى توصيف دقيق لهذه الطبيعة. هذا, فضلا عن الخلاف القائم حول تعريف القوّة بحدّ ذاتها. ويتوسّع النقاش, كذلك التباين في وجهات النظر, حول دور الدولة بشكل عام, ومحاولة قراءة النظريات المعروفة في العلاقات الدولية من ليبرالية وواقعية... في ضوء الواقع الجديد.

وترتبط بهذه الأنشطة, لا سيما غير الشرعية منها, مسألة دقيقة, تتصل بصعوبة معرفة القائم بها, وثانيا العجز عن إسناد الفعل الى فاعل واضح ومعروف, مع ما يستتبع ذلك, من عدم القدرة على تحديد المسؤول, ومعاقبته.

وهذا يقود الى السؤال عن المرجعيات القانونية المطلوبة لذلك, وما اذا كانت المعاهدات والاتفاقيات القائمة, لا سيما تلك المدرجة تحت عنواني قانون الحرب والقانون الدولي الانساني, صالحة للتطبيق, في مجال ذي طبيعة خاصة ومميزة. وبالرغم من اتجاه غالب, يؤكد على صلاحيتها, مع أنه لم يرتق بعد الى مستوى الإلزام, فإن مسائل عدّة هامة وحيوية, تستدعي معالجة على حده.

وفي هذا السياق, اختلفت التوجّهات بين الدول, حول ضرورة وضع معاهدة أم لا, خاصة بالفضاء السيبراني, شأنه شأن المجالات الأخرى, تنظّم قواعد التعامل فيه, وتحدّد الحقوق كما الواجبات, كذلك المسؤوليات والعقوبات. وهذا يطرح تحدّيا أمام الدول, لجهة وجوب التعاون فيما بينها, لتحقيق مصلحة مشتركة من جهة, ودفع مخاطر متفاوته الحجم, تترتّب على محاولات التفرّد والاستئثار ؟؟؟ من جهة ثانية.

ويأتي في عدادها, الفجوة الرقمية بين دول الشمال والجنوب, والانخراط في سباق محموم, نحو التسلّح السيبراني.

ولقد طرحت في رسالة بحثي هذه, الإشكالية التالية: الى أي مدى يمكن القول, أنّ التطوّر التكنولوجي, قد أوجد قوّة جديدة, تتنافس الدول, لا سيما الكبرى منها, على امتلاكها, وبالتالي توظيفها لتحقيق مصالحها؟ وهل هناك من نيّة لدى هذه الدول في وضع ضوابط لهذه القوّة؟

ولهذا الغرض, قسّمت رسالة بحثي, الى قسمين:

في القسم الأول, الذي يتضمّن فصلين, أتناول فيه, الإطار النظري المتعلّق بالتعريفات المتعدّدة التي طاولت مفهوم الفضاء السيبراني, والجدل الأكاديمي القائم, حول ايجاد تعريف محدّد لهذه الظاهرة الحديثة في العلاقات الدولية, والخصائص التي تجعل من هذا الفضاء ميداناً يتميّز به عن الميادين التقليدية للصراع, وذلك في المبحث الأول من الفصل الأول. أما في المبحث الثاني منه, فأناقش مدى ملائمة نظريات العلاقات الدولية:الواقعية, والليبرالية, والبنائية, للتحدّيات التي أوجدها الفضاء السيبراني.

أما في الفصل الثاني, فأطرح, بعد تقديمي للإطار النظري لمفهوم القوّة, في المبحث الأوّل, الحجج التي جعلت القوة تتحوّل من المفهوم التقليدي الصلب, الى قوّة ناعمة, فذكيّة. وأوضح في المبحث الثاني, أهمية التكنولوجيا في خلق القوة السيبرانية, التي تحمل الوجهين الصلب والناعم معا, الى حد يمكن اعتبارها قوة ذكية.

أما القسم الثاني, فأتطرّق فيه الى "سيادة الدولة" في الفضاء السيبراني, في ظل توافر القوّة السيبرانية في أيدي لاعبين من غير الدول, ما يطرح إشكالية عدم تماثل القوى من جهة, ومن جهة أخرى منافسة الأفراد والجماعات للدولة في امتلاك القوة, وذلك في المبحث الأوّل من الفصل الأوّل. أما في المبحثين الثاني والثالث منه, فأبيّن هاجس "الحرب السيبرانية", بين جازم باندلاعها, ومقلّل من خطورتها, اضافة الى الجوانب المتعلّقة بالسلاح السيبراني, من تعريفٍ له, الى أنواعه, ومزاياه, وخطورة استخدامه في العمليات السيبرانية. كما أبرز في المبحث الرابع منه, هوية اللاعبين من غير الدول, مبيّنة ما لتوظيفهم له من مزايا, وما يترتّب عليه من مخاطر.

وأوضح في الفصل الثاني, المنافسة القائمة بين الدول الكبرى, المالكة لهذه القوة السيبرانية, واستراتيجياتها المتبعة التي تظهر قوتها الهجومية أو الدفاعية, والاتجاه الواضح نحو عسكرة الفضاء السيبراني, وذلك في

المبحث الأوّل منه. لأنهي المبحث الثاني, بالإشارة الى المساعي المبذولة, لتحقيق التعاون بين الدول, سعياً منها لوضع ضوابط للقوّة, واستخدماتها في الفضاء السيبراني.

القسم الأول:الفضاء السيبراني ظاهرةٌ حديثةٌ في العلاقات الدولية

الفصل الأول: بروز الفضاء السيبراني في العلاقات الدولي

المبحث الأول: الفضاء السيبراني : تعريفاتٌ وخصائص

المبحث الثاني: السيبرانية والعلاقات الدولية: الحاجةُ الى إعادةِ تموضعِ النظريات التقليدية

الفصل الثاني: القوّة ما قبل الفضاء السيبراني وما بعده

المبحث الأول: التحوّل في القوّة: تراجعُ الصلبةِ منها لصالح أنماط جديدة

المبحث الثاني: التكنولوجيا وأثرها في تحولات القوة

القسم الثاني: لاعبو الفضاء السيبراني: تنافسٌ غير متكافئ وتعاونٌ محدود

الفصل الأول: تعددية اللاعبين وتنوّع الاستخدامات

المبحث الاول: الدولة في الفضاء السيبراني : تحدٍ للسيادة

المبحث الثاني: السايبر: الحرب القادمة

المبحث الثالث: السلاح السيبراني

المبحث الرابع: اللاعبون من غير الدول في الفضاء السيبراني

الفصل الثاني: مجالات توظيف الفضاء السيبراني

المبحث الأول: تصاعد التنافس الدولي

المبحث الثاني: تعاون دولي غير مقونن

القسم الأول: الفضاء السيبراني ظاهرة حديثة في العلاقات الدولية

لقد تعدّدت المجالات التي مارست فيها الدول, منذ القدم وحتى اليوم, لبعض الضغوط المتبادلة, ورسمت فيها ايضا حدودا للتعاون. وقد ظهرت هذه المجالات تباعا. وبفضل عوامل عدة. لعلّ من أبرزها الوسائل والأدوات. وقد اعتبر الفضاء السيبراني أحدثها, وربما الأكثر فرادة. وتعدّدت وجهات النظر حول تعريف هذا الفضاء السيبراني, فمنها ما ربطه بشبكة الانترنت فقط, ومنها ما قلّل من أهمية العنصر البشري فيه. ولكن الاتفاق سائد على أن الفضاء السيبراني هو ميدانٌ خامس بخصائص جديدة, ليس أقلّها الغموض, والتشبيك, والافتراضية, والتمدّد.

ظاهرة الفضاء السيبراني هذه, فرضت تحدّيات كبيرة للنظريات التفسيرية للعلاقات الدولية, في ظلّ ما أحدثته من إعادة ترتيب وتوزيع لأنماط القوى, مما فرض إشكالية التكيّف أو التغيّر حيال تفسير الواقع الدولي الذي فرضته هذه الظاهرة. فلقد أصبح للتقدّم التكنلوجي دوراً كبيراً في التأثير على قوّة الدول وحركتها الخارجية, محدثة ثورة أسماها البعض بالثورة الصناعية الثالثة.

ونظراً لما للمعلومة من أثر هام فى حسم الصراعات الدولية، كان جدير بالملاحظة, معرفة أثر التكنولوجيا الحديثة, والفضاء السيبراني على مفهوم القوة وخصائصها وتحولاتها، فأشكال القوة تتغير بتغيّر التكنولوجيا، وقد أثّر الفضاء السيبراني على الأشكال التقليدية للقوة، وطرح مفهوم وشكل جديد هو القوة السيبرانية.

الفصل الأول: بروز الفضاء السيبراني في العلاقات الدولية

قديما, كان النشاط البشري محصورا في البرّ والبحر. فقد مكّنت التكنولوجيا الإنسان من الاستفادة من البرّ , عبر العجلات, والعربات الحربية, والدبابات . ورأى ***ماكيندر Mackinder*** في سكك الحديد, قدرة للدول في أن تلعب دورا عالميا. ففي نظريته, "قلب الأرض", أجرى مقارنة بين الأمم التي تسيطر على قلب أوراسيا, مثل المانيا وروسيا, والأمم التي تعمل على الأطراف, كانكلترا والولايات المتحدة, حيث لاحظ مدى مساهمة التطوّر في التصنيع والتكنولوجيا, مثل سكك الحديد والتلغراف, في وتيرة وحجم العمليات العسكرية .واعتبر أنّ استخدام الأمم الموجودة في "قلب الأرض", لوسائل النقل, وتكنولوجيا

الاتصال, سيمكّنها من إنشاء خطوط دفاع, والقيام بعمليات عسكرية سريعة, في المناطق التي تختارها. فكتب:" إنّ الذي يحكم شرق أوروبا يسيطر على القلب, والذي يحكم القلب يسيطر على جزر العالم, والذي يحكم جزر العالم يسيطر على العالم بأكمله".[١]

كما مكّنت التكنولوجيا الانسان, من استخدام المجال البحري , للسيطرة على الممرات البحريّة, لأغراض حربيّة, وتجاريّة. ففي عام ١٨٩٠, وضع ***الفرد ماهان Alfred Thayer Mahan***, الخطّة الإستراتيجية للبحرية الأمريكية, للقرن العشرين, والتي ساهمت في الإنتصار الذي حقّقته الولايات المتحدة الأمريكية, في الحرب العالمية الثانية[٢]. وفي هذا السياق, أقدم الرئيس الأميركي, ***ثيودور روزفلت Rososevelt Theodore*** , على تطوير البحرية الأميركية, ونشرها حول العالم, عام ١٩٠٧ . لكن التغيير الأساسي تمّ في القرن العشرين, حيث وضع منظّرون أمثال ***غراي,وسلون, وهارت Gray,Sloan,Harte*** نظرياتهم حول القوّة الجويّة, وقدرتها على تحقيق ضربات مباشرة ضد العدو, دون الحاجة الى غزو الجيش للحدود, ما دفع الرئيس الأمريكي, ***فرانكلين روزفلتFranklin Roosevelt***,الى الإستثمار في القوّة الجوية, خلال الحرب العالميّة الثانية.[٣]

وفي الستينيات من القرن الماضي, وبعد تطوير الصواريخ العابرة للقارات, والأقمار الصناعية, توسّعت النشاطات البشرية لتشمل الفضاء الخارجي, وبدأت النظريات تظهر حول أهمية القوّة في المجال الفضائي, ما جعل الرئيس الاميركي, ***جون كينيدي Jhon F.Kennedy*** , يرسل أول رجل الى القمر, ويطلق برنامجا يضمن من خلاله, قيادة أميركا للفضاء. [٤]

وفي عام ٢٠٠٩, ومع تنامي ظاهرة الإنترنت, والشبكة العالمية, وزيادة فرص تبادل المعلومات, و الإتصال الرقمي اللاسلكي, دعا الرئيس الاميركي , ***باراك اوباما Barak Obama*** , الى مبادرة جديدة

---

[1] G. J Rattray. (2009). An environmental approach to understanding cyberpower. *Cyberpower and National Security,ch10,p:5-8*

[2] http://defense-arab.com/vb/threads/22086/

[3] Nye Jr, J. S. (2010). *Cyber power*. HARVARD UNIV CAMBRIDGE MA BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS. p:4

[4] Ibid,p:4

في القوّة الفضائية, بعد أن أصبح الفضاء السيبراني, يشكل الحقل الخامس للنشاط البشري[5]. وهذا يعني , وفقا ***لجوزيف ناي Joseph Nye*** , أنه كلما بدّل التطوّر التكنولوجي في شكل القوّة, كلما استجاب القادة السياسيون لذلك.

ولقد قطع مفهوم الفضاء السيبراني, طريقا طويلا ,منذ ولادته في عالم الخيال العلمي في أوائل الثمانينات,[6] حتى بات, خلال ثلاثة عقود, يصنّف عسكريا كميدان جديد للصراع. أمّا اجتماعيا, فلقد أصبح يشكّل بيئة , للنمو الاقتصادي. واليوم, يكاد يوجد في كل النواحي الحياتية للمواطن, من سبل جنيه للمال, الى كيفية بنائه لعلاقات إجتماعية, الى إثرائه فكريا وثقافيا .فما هو الفضاء السيبراني, وما هي خصائصه؟

---

[5] http://www.washingtonpost.com/wp-dyn/content/article/2009/05/29/AR2009052900350.html (last retrieved august,4,2016)

[6] العبارة وردت في "Burning chrome" ل William Gibson, ثم أطلقت في روايته "Neuromancer", "1984

المبحث الأول: الفضاء السيبراني: تعريفاتٌ وخصائص

شأنه شأن أي مفهوم, شهد الفضاء السيبراني, مقاربات مختلفة, إن لجهة تحديده, أو لجهة تبيان خصائصه.

المطلب الأول: الفضاء السيبراني وجدليةُ التعريف

انبثقت عبارة "***cyber***", من *أعمال* ***نوربرت واينر Norbert Weiner***, الذي قدّم تعريفا لعبارة "***cybernetics***", في كتابه " التحكّم والاتصال في الحيوان والآلة", مفاده أنّ التفاعل بين الانسان والآلة, يؤدي الى خلق بيئة بديلة للاتصال, تشكّل البنى الأساسية لمفهوم الفضاء السيبراني.[7]

وفي أوائل الثمانينيات, صاغ الكاتب ***وليام غيبسون William Gibson***, عبارة "***cyberspace***", في روايته "***Neuromancer***" . ورغم أن العبارة قد وضعت في سياق الخيال العلمي, الاّ أنّها أصبحت تستخدم بشكل واسع بين الأكاديميين, والمتخصّصين في هذا المجال. ففي كتابه هذا, وصف ***Gibson*** , الفضاء السيبراني, بأنّه "هلوسة رضائية, يمارسها يوميا بلايين المستخدمين في كلّ الأوطان ... فهو تعقيد فاق التصوّر". وأضاف, إنّه "عالم حيث الناس يتّصلون ماديّا, ويسعون لإكتشافة, إنه وعي مجرّد من الماديات".[8] وعنده, أنّ الفضاء السيبراني , ليس فضاء بيانات ساكنة, ولكن قنواته الاتّصالية تصل العالم الحقيقي, وتتيح لملّاحي هذا الفضاء, سبل التفاعل مع ذلك العالم. ليعود ***غيبسون*** ويقول عنه, "بدا ككلمة طنّانة فعلا, تخلق انطباعات, لكنها جوهريا بدون معنى. كما أنها تولّد ايحاءات, لكن من دون أية دلالة سيميائية."[9]

---

[7] Wiener, N. (1961). *Cybernetics or Control and Communication in the Animal and the Machine* (Vol. 25). MIT press.

[8] Gibson, W.(2000) . *Neuromancer*. Penguin.

[9] "No Maps for These Territories". Docurama.com. (Retrieved august 10,2016)

وفي أوائل تسعينات القرن الماضي, وضع ***جان بيري بارلو*** ***John Perry Barlow*** العبارة , كمفهوم معاصر, في سياق وصفه للعلاقة بين الكمبيوترات, وشبكات الاتصال السلكية واللاسلكية, في مقالة أعلن فيها تأسيس منظمة الجبهة الالكترونية ***Electronic Frontier Foundation***, عام ١٩٩٠[10]. وقد وصف الفضاء السيبراني, بأنّه وطن بلا حدود, متحديّا بذلك فكرة الدولة القومية, التي قدّمها, ***آدم سميث***, ***Adam Smith***, مميّزا بذلك, بين عالم افتراضي وعالم واقعي.

كما وردت مصطلحات مشابهة, لباحثين آخرين; مثل تعابير: الوجود في اللاشيء "***being in nothingness***", و الوجود في مكان آخر "***being elsewhere***" ***(Meyrowitz)***, أو تعابير: الرسم المعلوماتي, "***infographical***" والفضاءات الافتراضية ثلاثية الابعاد "***three dimensional virtual spaces***"....(***Davidow***)

وتعيد ***نازلي شكري*** ***Nazli Choucri***, الأصول التاريخية والفلسفية لعبارة ***cyber***, الى "قصة الكهف" (Allegory of the cave) لأفلاطون في كتابه "الجمهورية" , حيث رأى, أننا نعيش في زمن الواقع الخيالي الذي نخدع في كونه حقيقة, وأن هذه الحقيقة, لا يمكن الوصول اليها, الاّ من خلال التدريب الفكري[11].

كما أن ***لديكارت*** ***Decartes*** فرضية مماثلة, مفادها أن البشر قد يخدعون بواسطة "شيطان" يمدّهم بحقائق زائفة, وأن الحقيقة الوحيدة, تكمن في فكر وعقل الانسان[12].

ولقد استخدم فلاسفة الإغريق ال ***cybernetic***. فالكلمة ***cyber*** تشتق من الفعل اليوناني ***kubernao***, الذي يعني "يقود "***to steer***", وهو جذر الكلمة الحالية, "يحكم أو يتحكّم في "***to govern***" . وتطلق السيبرانية ***cybernetic*** , اسما لعلم الاتصالات, والمعلومات, والتحكّم. لذا تشمل

---

10 Barlow, J. P. (1990). *Crime & Puzzlement*. Electronic Frontier Foundation.Electronic Frontier Foundation (pp. 44-48)

11 Choucri, N. (2012). *Cyberpolitics in international relations*. MIT Press. *Cyberpolitics in international relations*.MIT Press. P:7

12 http://www.newworldencyclopedia.org/entry/Cyberspace

الكلمة المعنيين اللصيقين بهذا المعنى, "الملاحة **navigation** "عبر فضاء من البيانات الالكترونية, اضافة الى التحكّم الذي يتحقق عبر معالجة تلك البيانات.[١٣]

وينظر كلّ من ***مورنينغستار و فارمر*** ***Chip Morningstar و F. Randall Farmer***, الى الفضاء السيبراني, على أنّه الانخراط في التفاعل الاجتماعي, أكثر من كونه تطبيقا تقنيا فحسب. فهو يؤمّن بيئة, تتألّف من مشاركين متعدّدين, قادرين على التأثّر والتأثير ببعضهم البعض. وقد استخلصا هذا المفهوم, من المقاربة التي ترى, أنّ البشر يبحثون عن الغنى, والتعقيد, والعمق. في عالم افتراضي.[١٤]

فيما بعد, قدّمت عدّة تعريفات للفضاء السيبراني. فالقاموس العسكري لوزارة الدفاع الاميركية,عرّف "الفضاء السيبراني" بأنّه," حقل عالميّ في بيئة المعلومات, المؤلّفة من شبكة مترابطة من البيانات والبنى التحتية لتكنولوجيا المعلومات, تضمّ ,فيما تضم, شبكة الإنترنت, وشبكات الاتصال, والحواسيب, وأنظمة المعالجة, و التحكّم." [١٥] ولكن هذا التعريف, ينقصه العنصر البشري, الذي أعطاه كلّ من ***غيبسون وفينر***, أهمية بارزة في تعريفهما للفضاء السيبراني.

أمّا المفوّضيّة الأوروبية, فتعرّف الفضاء السيبراني, بأنّه" الفضاء الإفتراضي الذي تدور في فلكه البيانات الالكترونية للحواسيب العالمية". لكنّها ايضا غيّبت العنصر البشري, وحصرت تعريفها للفضاء السيبراني, في البيانات التي تنتقل بين الحواسيب العالمية.

وترى فيه الموسوعة الالكترونية ***webopedia*** , "استعارة لوصف الأرضية الغير مادية التي تخلقها أنظمة الحواسيب"[١٦].

أما ***Wikipedia*** , فتعرّف الفضاء السيبراني بأنّه "الدخول الى المجال الكهرومغناطيسي العالمي, واستخدامه عبر التكنولوجيا الالكترونية, والطاقة الكهرومغناطيسية, للتمكّن من الاتصال والسيطرة"[١٧].

---

[13] Principia Cybernetica "Cyberspace"http://pespmc1.vub.ac.be/cybspace.html

[14]GAILE-SARKANE, E., & ŠČEULOVS, D. Cyberspace vs. Electronic Environment: The Case of Europe.p3

[15] Pub, J. (1994). Pub 1-02. *Department of Defense Dictionary of Military and Associated Terms*, *23*.P:64

[16] http://www.webopedia.com/TERM/C/cyberspace.html

[17] https://en.wikipedia.org/wiki/Cyberspace

ويعرّفه **كويل *Kuehl* ,** بأنّه" ميدان عالمي, في بيئة المعلومات, حيث ظهرت ميزته الخاصة والفريدة, باستخدام الالكترونيات والمجال الكهرومغناطيسي, من أجل خلق, وتخزين, وتغيير, وتبادل, واستغلال المعلومات عبر شبكات متصلة ومترابطة,باستخدام تكنولوجيا المعلومات والاتصال."[١٨] وبرأيه , إن "شبكات المعلومات هذه, تقيم في الفضاءين المادي والافتراضي معا, وفي داخل وخارج الحدود الجغرافية للدول, وإنّ مستخدميها يتراوحون بين دول, وأفراد, ومجموعات عبر– وطنية, لا تنتمي الى دولة معينة, أو منظّمة تقليدية". كما تعتمد هذه الشبكات على أبعاد ثلاثة:

- العمليات المعلوماتية, أي المجال المادي والبنى التحتية,التي تؤمّن الإتصال, وأنظمة المعلومات, والشبكات, والمستخدمين لها.
- المضمون, الذي يمكن إرساله رقميا والكترونيا,الى أي مكان, وفي أي وقت تقريبا.
- الإدراك البشري, الذي ينجم عن هذا " المضمون", والذي يؤثّر بقوة على سلوك البشر, وطريقة اتخاذهم للقرارات.[١٩]

وقد عرّفه ***علي رحوّمة***, في كتابه "علم الإجتماع الآلي", أنّه "قناة رقمية إلكترونية داخل مسافات متشابكة من خطوط, وقنوات اتصال معدنية, وضوئية, وهوائية, في شبكة الشبكات, أي "الإنترنت". ويشار اليه تكنولوجيا, بأنّه طريق للمعلومات فائق السرعة, متمدّد, ومتّسع لمساحات هائلة من الانطلاق الحركي المتواصل, في آليات تفاعلية للعقول الانسانية, والحاسوبية بأنواعها. ومن خلال هذا الفضاء, يحدث التفاعل البشري الآلي, عقليا, ونفسيا, واجتماعيا, بمختلف الحواس الانسانية, وكذلك الالية. وفي هذا الفضاء ايضا, يتشكّل مجتمع الانترنت, متكونا من أعضائه الكونيين ,الأفراد,و الجماعات البشريين, في علاقاتهم بعضهم ببعض, بمختلف الخصائص, التي تفرضها هذه البيئة الانسانية الآلية".[٢٠]

وبالنسبة لكلّ من ***بيتز وستيفنز David J. Betz & Tim Stevens,*** إن ايجاد تعريف له, ليس أمرا بدون أهمية, لأن ما نشمله في التعريف, أو نستبعده , له دلالاته في كيفية استخدام القوة, والتي تحدّد

---

18 Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. *Cyberpower and national security,* p:26

19 Ibid p:4

20 علي محمد رحومة,"علم الاجتماع الآلي,سلسلة عالم المعرفة, المجلس الوطني للثقافة والفنون والآداب,الكويت ٢٠٠٨, ص١٢٤

استراتيجيات الفضاء السيبراني , واستخدام القوة السيبرانية. وفي هذا الاطار, قدّما مفهومين أساسيين للفضاء السيبراني: الأوّل يستبعد البنى التحتية, والثاني يشملها. فالأوّل, وهو" النموذج الحصري", يقدّم الفضاء السيبراني, وكأنّه الفضاء مقيما بين مكونات أجهزة شبكات الكمبيوتر.فهو ليس فضاء بالمعنى الجغرافي التقليدي, إنّما تجربة الوجود في الفضاء السيبراني, وكأنها تمتلك الكثير من مزايا العالم المادي, ولو فقط من خلال الجمع والتماثل. اذا, الفضاء السيبراني, هو المكان على الشاشة, وبعيدا عنها. فهو الفضاء الموجود في الأسلاك وفي الهواء ,حيث الاتصالات بين البشر, تتم من خلال نقل ***البيتات bits.*** فالفضاء السيبراني موجود في عقول المستخدمين, والحدود غير واضحة, بين ما هو حقيقي وما هو فعلي". أمّا الثاني, فهو " النموذج الشامل" ومشتقّاته, الذي يتضمّن البنى التحتية اللازمة, للوصول الى الفضاء الاجتماعي للفضاء السيبراني. فالطبقة الاجتماعية, هي مجرد الطبقة العليا, من نموذج لطبقتين او اكثر. وهذا النموذج يتألف من طبقة معلومات "افتراضية", مركّبة فوق طبقة مادية من الأجهزة.[٢١]

ويعتبر كلّ من ***نيكيتاكوس ومافروبولوس N. Nikitakos and P. Mavropoulos***, أنّ تعريف الفضاء السيبراني, بأنه الفضاء الذي يتضمّن البنى التحتية, التي يمكن الوصول إليها عبر الإنترنت, هو تعريفٌ محدود, لأنّه ليس الإنترنت فحسب, رغم كونها الأشهر, والأبرز, وتشكّل الجزء الأكبر لهذا الفضاء. كما أن هذا التعريف, يستبعد ما يسمّى بالحرب السيبرانية, التي تتعامل مع نظم معزولة, وتتطلّب فجوة هوائية ***air gap***, بينها وبين سائر العالم, وبالتالي غير معرّضة للحقل الكهرومغناطيسي الخارجي, حيث يمكن الوصول اليها من خلال وسائل أخرى. وتعدّ الصيانة الشاملة لسلسلة الإمداد, أهم تلك الوسائل. فالطريقة الوحيدة للتأثير على هذه النظم, هي عبر استهدافها ببرمجيات خبيثة على شكل ***logic bombs***قنابل منطقية, وشرائح مبرمجة ***programmed chips***, والتي يتم تشغيلها, عندما تستوفي شروطا معيّنة. فالفضاء السيبراني, هو الفضاء الذي لا يقتصر على الإنترنت, إنما يتضمّن شبكات معزولة. فكل النظم الصناعية متصلّة بشبكة الإنترنت, أو بشبكات معزولة, من خلال نظم التحكّم الإشرافي[٢٢], وتحصيل البيانات المعروف ب ***SCADA***[٢٣].

---

[21] Betz, D. J., & Stevens, T. (2011). Chapter One: Power and cyberspace. *Adelphi Series*, *51*(424), 35-54. 37-38

[22] CARAYANNIS, E., Campbell, D. F., & Efthymiopoulos, M. P. (2014). *Cyber-Development, Cyber-Democracy and Cyber-Defense* (pp. 279-301). Nueva York: Springer.

ويضيف ***لورنتس lorents*** [٢٤], الى تعريف الفضاء السيبراني عنصر "الوقت", بحيث يصبح تعريفه, كالآتي: " هو مجموعة من أنظمة المعلومات, تعتمد على الوقت, وتتصل فيما بينها, بوجود العنصر البشري المتفاعل معها".

ويعود تعدّد التعريفات, الى تعدّد وجهات النظر, حول الفضاء السيبراني. اذن, لا يوجد تعريف مشترك حوله, ومعظم التعريفات المستخدمة, ينقصها أحد العناصر. ولكن تتفّق على نواة المفهوم, أي أنه شبكة عالمية من الأجهزة, والبرمجيات, والبيانات المتصلّة بعضها ببعض. بالإضافة الى عامل هام, هو وجود العنصر البشري, الذي يتواصل عبر هذا الفضاء, وبالتالي يصبح جزءا منه.

ولعل التعريف الأقرب الى الواقع هو الذي توجه ***فريد سكريير Fred Schreier*** , بقوله:" أنّ الفضاء السيبراني هو عبارة عن أنظمة معلومات متشابكة ومتصلة, تسكن في الفضائين المادي كما والافتراضي, في داخل وخارج الحدود الجغرافية, تضم مستخدمين من دول, ومؤسسات تابعة لها, إضافة الى مجتمعات, وأفراد, ومجموعات عبر قومية, لا تعلن ولاءها لأية منظّمة تقليدية, أو كيان وطني. هي تعتمد على أبعاد ثلاثة, مختلفة لكن مترابطة: مادية, ومعلوماتية, ومعرفية, تؤلف معا بيئة المعلومات العالمية, أي المنصّة المادية, وهي الأنظمة والبنى التحتية التي تؤمّن الاتصال العالمي لربط أنظمة المعلومات, والشبكات والمستخدمين بعضهم ببعض. هذا إضافة الى الكم الهائل من محتوى المعلومات, التي يمكن إرسالها رقميا وإلكترونيا, الى أي مكان, وفي أي وقت, والى أيّ كان. وأخيرا, الإدراك البشري, الذي ينجم عن زيادة في الوصول الى المحتوى, والذي يمكن أن يكون له تأثير كبير, على سلوك الانسان وصنع القرار. [٢٥]

---

[23] SCADA Supervisory control and data acquisition: اختصار لنظام التحكم الاشرافي وتحصيل البيانات, وهي تشير الى أنظمة التحكّم الصناعي وهي نظام حاسوبي للمراقبة والتحكم في العمليات في العديد من المصانع والشركات الكبرى, فعلى سبيل المثال يستخدم في مراقبة خطوط البترول وخطوط المياه او الغاز او في معامل الافران واجهزة التكييف ومصانع الاسمنت والحديد. وتتم المراقبة من خلال وجود حساسات متصلة بجهاز الحاسوب المركزي, وانظمة تحكم طرفية موجودة على قنوات النقل او الخزانات.

[24] Ottis, R., & Lorents, P. (2010, April). Cyberspace: Definition and implications. In *International Conference on Information Warfare and Security* (p. 267). Academic Conferences International Limited.

[25] Schreier, F. (2015). *On cyberwarfare*..P:11

المطلب الثاني: السيبراني ميدانٌ خامس بخصائص مميّزة

يرى كلّ من ***نازلي شكري ودايفيد كلارك Nazli Choucre, David Clark*** , أنّ الفضاء السيبراني, كان يعتبر الى وقت قريب, من مسائل السياسات الدنيا ***Low Politics*** , وهي عبارة تستخدم للدلالة على الشؤون الحياتية الإجتماعية, والإقتصادية, التي لا تؤثّر, بشكل جذريّ, في استقرار الدولة . أما اليوم, فالفضاء السيبراني, أصبح من مسائل السياسات العليا ***High Politics***. فممارسات كقطع الإنترنت, في فترات عدم الإستقرار السياسي, أو الأمني لدولة ما, أو تسريب وثائق حكومية سريّة عبر ***Wikileaks*** , أو هجوم سيبراني ترافق مع أحداث استونيا وجورجيا, أو الهجوم السيبراني لتقليص القدرة الإيرانية النووية, كلّها أمثلة, تدل على أنه لا يمكن تجاهل وجود وقدرات الفضاء السيبراني .[٢٦]

ففي الفضاء السيبراني, كما في ميداني الجوّ والفضاء, كلّ النشاطات تتطلّب استخدام التكنولوجيا. وهو يتمتع بخاصية فريدة, وهي أن التفاعل محكوم بالبرامج والأجهزة, التي هي من صنع الإنسان. لذا, فإن "جغرافيا" الفضاء السيبراني أكثر تقلّبا, من البيئات الأخرى. ففي الوقت الذي يصعب فيه تحريك الجبال والمحيطات, يمكن تشغيل أجزاء من الفضاء السيبراني, أو إغلاقها بكبسة زر, بحيث يمكن إيجادها أو تحريكها , بإدخال تعليمات مشفّرة, بجهاز التوجيه (***router***) أو التبديل (***switch***). لكنّ الفضاء السيبراني, ليس طيّعا دائما. فسرعة ونطاق التغيير, تتعلق بقوانين فيزيائية, وخصائص الشيفرة, وقدرات المنظمات والأشخاص.[٢٧]

وبحسب نشرة صادرة عن السلاح الجوي الاسترالي, فإنّ للفضاء السيبراني أربع خصائص:

فقرة أولى: التشبيك *inter-connectivity*

يتألف الفضاء السيبراني, من أنظمة مادية تتصل ببعضها البعض, قد تختلف في التفاصيل, ولكن تشترك فيما بينها, في كونها البنى الأساسية, للنظام المادي المتصل بها. فعالم الطيران, مثلا ,هو عالم ماديّ, وقوّته تعتمد على أنظمة فردية كالمنصّات والقواعد, للعمل كمجموع متكامل لأنظمة متعدّدة. لكن

[26] Choucri, N., & Clark, D. (2011). Cyberspace and International Relations: Toward an Integrated System. *Massachusetts Institute of Technology, Cambridge, Massachusetts*.208-25.

[27] Rattray, G. J. (2009). An environmental approach to understanding cyberpower. *Cyberpower and National Security*, 253-274.*p:7*

الفضاء السيبراني, يشكّل بحدّ ذاته نظاما متكاملا, نظرا للإتصال البيني لأنظمة مادية متعددة. وهذه الخاصية, هي ما تحدّد الفضاء السيبراني, وهي التي سمحت للكثير من التطبيقات , في جذب ملايين المستخدمين, كالفيسبوك, مثلا, في فترة زمنية قصيرة. ولكنها جعلت منه, في الوقت عينه, عالما معقدا, من الصعب تعريفه أو فهمه, خالقا لتحديات في المجالين القانوني القضائي. فقد يمتلك الأفراد, والشركات, بعضا من هذه الانظمة المادية, ولكن لا توجد ملكية جماعية للفضاء السيبراني ,مما يجعل الولوج الى هذا العالم أقل تعقيدا, وأقل تكلفة. كما أن مستخدمي هذا القطاع, يسعون الى ممارسة النفوذ, والتأثير فيه, من خلال الإستغلال الأقصى للموارد المتوافرة فيه, باستثمار بسيط جدا. [٢٨]

فقرة ثانية: الإفتراضية *virtuality*

يعرّف قاموس ***أوكسفورد Oxford*** , الفضاء الالكتروني بأنّه "وجود غير ماديّ, لكن أنظمة الكمبيوتر جعلته يبدو كذلك من وجهة نظر مستخدميه. هو عالم اصطناعي, خلق بواسطة تكنولوجيا الكومبيوتر, المتفاعلة بين بعضها البعض".[٢٩] ومع أنّ الفضاء السيبراني, يتألف من أنظمة ماديّة , لكن ليست كلّها محسوسة, لأن بعض طرق الإتصال هي لاسلكية, وتستخدم المجال الكهرومغناطيسي. فطبيعة الفضاء السيبراني الإفتراضية , وعالمه الغير محدود , لا تسمح القيام بتحرّكات مادية في داخله, إنّما بأفعال, حيث يتم نقل المعلومات لا القيام بالتحرّك جسديا.ومع أن كلمة "افتراضي" , قد تستخدم كمرادف لكلمة "حوسبة""computing" , لكنها تعني عادة, أنّ الأجسام الإفتراضية, هي نوعاً ما, من نسج الخيال. كما أن خاصية البرمجة التي يمتلكها الفضاء السيبراني , تجعل من الممكن لشخص واحد, أن يكون له تأثير هائل, من خلال برامج تسمح له أن يعمل افتراضيا, مثلا, أن يبدو وكأنه موجود في أماكن متعددة. كما يمكن لفرد واحد استنساخ نفسه بشكل برنامج, والعمل على مستوى عالمي, كاطلاق الفيروسات في الحواسيب.

---

[28] http://en.oxforddictionaries.com

[29] **http://airpower.airforce.gov.au/publications/Details/454/157-What-is-Cyberspace-Examining-its-Characteristics.aspx**

فقرة ثالثة: التمدّد *expansion*

"تتمدّد المعلومات في المجال السيبراني وتتطوّر, كلما اتخذ مستخدم اجراء, قد يدخل تغيرات طفيفة في هذا المجال, تمكّن المستخدم القادم من استعمالها"[٣٠] . فالطلب يتزايد على المعلومات في الفضاء السيبراني, ما يفرض توسّعا وتطوّرا مماثلين, للنظم الفيزيائية والتكنولوجية التي تعتمد عليها. والمجال السيبراني نفسه, ينمو ويتطوّر, كلما تطوّرت تكنولوجيا المعلومات, وكلما توسّع السوق, وازداد الطلب, ما ينعكس على جوانب كثيرة منه, ويدفع نحو نظام يسمح بالابتكار السريع. ولتحقيق ذلك, لا بد من ضمان الاتصال, والقدرة على الوصول الى أو ايصال البيانات. هذه الفلسفة هي توسعية بطبعها, وينتج عنها إعادة تعريف مستمر للفضاء السيبراني, من خلال طبيعة الاعمال التي يقوم بها المستخدمون. وهذا يتعارض مع الطبيعة الفيزيائية, الثابتة لمجالات الجو والبحر والبر.

فقرة رابعة: الغموض *Ambiguity*

إن المزج بين العناصر المذكورة سابقا, يجعل الفضاء السيبراني غامضا, ومعقدا, وصعب الفهم. وقد يكون السبب, سعة المعلومات المتوافرة فيه. فحجم التخزين, وكمية البيانات, واستخدامات هذا المجال, تخلق آثارا قانونية معقّدة وصعبة التحديد, ما يزيد في غموض الفضاء السيبراني.[٣١]

ويركّز كلّ من ***نازلي شكري ودايفيد كلارك*** على خاصية الإنترنت, في إعطاء نموذج من أربع طبقات, لوصف خصائص الفضاء السيبراني, مع تأكيدهما على إمكانية تعميم هذا النموذج, على نواحي الفضاء السيبراني الأخرى, مثل منصّات الحوسبة وأنواع أخرى من الشبكات.

وهذه الطبقات, تتدرج من الأعلى الى الأسفل, كما يأتي:

- البشر, أي المستخدمون, والمنخرطون في الفضاء السيبراني, الذين يتواصلون ويتعاملون مع المعلومات, والذين يتّخذون القرارات, وينفّذون الخطط, و يساهمون في إدخال التغييرات, اليه.
- المعلومات بأشكالها المختلفة, والتي تخزّن, وتنقل, فيه.
- اللبنات المنطقية, التي تؤمّن التقديمات, وتدعم بنيته.

---

30 Winner, J. L., Holt, L. S., Duran, J., & Watz, E. (2010). *Cyber Operations Virtual Environment*. LUMIR RESEARCH INST GRAYSLAKE IL.

31 Airpower.airforce ,opcit p:2

- الأسس المادية, التي تدعم اللبنات المنطقية, والتي من خلالها يتحقق التفاعل الإفتراضي. وهي عبارة عن مجموعة من أجهزة الكمبيوتر, والخوادم, والشبكات, وأجهزة الاستشعار, ومحولات الطاقة, حيث يتم الإتصال, عبر أسلاك أو ألياف, وعبر الإذاعة أو نقل فعلي لأجهزة الحوسبة والتخزين, من مكان الى آخر. وهذه قد تكون الطبقة الأسهل للفهم, لأنها محسوسة.

كما يعتبران , أن الحواسيب وحدها, لا تشكل ما نصفه بالفضاء السيبراني. انما التشبيك, هو ما يصنع هذا الفضاء, ويؤثّر, ويغيّر, أحيانا في طبيعة اللاعبين, ووظائف كل طبقة.[٣٢]

أما ***شلدون Sheldon***, فيرى أن الخصائص الرئيسة للفضاء السيبراني, تكمن في النقاط الآتية:

- الفضاء السيبراني يعتمد على المجال الكهرومغناطيسي. فبدون هذا المجال, تفقد تكنولوجيا المعلومات والاتصالات (ICT), القدرة على العمل.
- الفضاء السيبراني يتطلّب أجساما من صنع الانسان ,مقارنة مع ميادين البر, والبحر, والهواء, والفضاء الخارجي. فبدون الرقائق, والألياف الضوئية, وألواح إلكترونية... لا يوجد فضاء سيبراني. ولكن, لا يختفي الفضاء الخارجي, إن لم يتمكّن الانسان, من وضع الأقمار الصناعية في مدار الأرض, كما أنّ البحر سيبقى, سواء فشل الإنسان أم نجح, في السيطرة على فيزياء تعقيدات الطفو. كذلك الأمر بالنسبة للهواء, سيستمر في الوجود, إن لم يتم اكتشاف مبادئ الطيران. فالفضاء السيراني, لم يكن ليوجد, إن لم يستطع الانسان أن يبتكر, ويصنع, التكنولوجيا القادرة على استغلال الخصائص المختلفة, للحقل الكهرومغناطيسي.
- تتوافر البدائل باستمرار, في الفضاء السيبراني. ففي الوقت الذي يوجد فيه ميدان واحد لكلّ من البرّ, والبحر, والفضاء, يمكن أن يتوجد العديد من الفضاءات السيبرانية. إذ يحصل مثلا, أن يتم تدمير طائرات العدو في ميدان الجو, ويحسم الامر. لكن في الفضاء السيبراني, عند اغلاق موقع إلكتروني للجهاديين, مثلا, تبقى أمام هؤلاء إمكانية فتح موقع جديد, بإسم مختلف, في ساعات قليلة, وعلى خادم آخر . والأمر نفسه ينطبق, على الشبكات التي يمكن إصلاحها, وإعادة بنائها, بفضل قلّة تكلفة الأجهزة وتوفّرها.
- إنّ الولوج الى الفضاء السيبراني, رخيص نسبيا. فكما يشير ***كول ستيفن كورنس Col Stephen Korns***, إنّ الكثير من الأسلحة السيبرانية, هي سلع يمكن شراؤها عن "الرف",

[32] Choucri & Clark,(2011) p: 12

بأسعار معقولة. فبرنامج "تعطيل الخدمة ", مثلا, يمكن تحميله على الكمبيوتر الشخصي, واستخدامه ضد الهدف المقصود.

- أسبقية الهجوم على الدفاع في الفضاء السيبراني, لأسباب متعددة , منها أنّ الهجوم يحدث بسرعة كبيرة , ومن أي مكان في العالم ,دون تحديد المصدر, أو المسؤول عنه .
- الفضاء السيبراني يتألف من أربع طبقات, والسيطرة على إحداها, لا يعني السيطرة على كلّ الطبقات: البنى التحتية, والبنى المادية, والطبقتان السيميائية والنحوية. فالسيطرة على البنى التحتية, لا تعني السيطرة على الطبقات الباقية, مع استثناء يتعلّق بما ينوي, اللاعب القيام به. فاذا كان المقصود تعطيل الشبكة, يكفي تدمير البنى التحتية ليصبح ذلك فعليا[٣٣].

ويرى كلّ من ***جيل رولاند, وماسون ريس, وسوجيت شينوي*** ***Jill Rowland, Mason Rice, Sujeet Shenoi***, أنّ العالم الافتراضي الذي أوجده الفضاء السيبراني, يستمد وجوده من العالم الماديّ, من أجهزة, وبرمجيات, وبيانات, ومن العنصر البشري, وكلّها تتطلّب موارد مادية (كالهرباء, والمباني, والاتصالات السلكية والاسلكية ...). وذلك يعني, أنّ الفضاء السيبراني, يستخدم الميادين الخمسة, من بحر, وبرّ, وجوّ, وفضاء خارجي, وفضاء سيبراني.

كما أن الكيانات السيبرانية, قد بدأت فعلا بالظهور في الكثير من الميادين. ***فغوغل Google*** ,على سبيل المثال, والذي تأسّس عام ١٩٨٨, هو إحدى الشركات الأكثر نجاحا ,في دعم الحضور الإفتراضي أو السيبراني, من أجل خلق أرباح فعلية في عالم الواقع. كما أنّ ***فيسبوك Facebook*** , هو تجسيد لشركة, تحقّق عائدات مالية هائلة, بمئات الملايين من المستخدمين, ولكن جذورها في الفضاء السيبراني.

أما الإنترنت, والذي هو كيان سيبراني آخر, مكوّن من بنى تحتية, ومن نظام إقتصادي ومالي, ومن مساهمين ,وزبائن, فهو كذلك قوّة لا يستهان بها, داخل وخارج الفضاء السيبراني[٣٤].

ويشكّل ويكيليكس ***Wikileaks*** ,نوعا آخر من الكيانات السيبرانية, العبر وطنية, والحاصل على مؤيدين كثر لإيديولوجيته. كما يظهر دعمه ***لإدوارد سنودن Edward Snowden***, مسرّب الوثائق السريّة

---

[33] Sheldon, J. B. (2011). *Deciphering cyberpower: Strategic purpose in peace and war*. AIR UNIV MAXWELL AFB AL STRATEGIC STUDIES QUARTERLY..p:96-98

[34] Rowland, J., Rice, M., & Shenoi, S. (2014). The anatomy of a cyber power. *International Journal of Critical Infrastructure Protection*, *7*(1), 3

لوكالة الأمن القومي الاميركية, والهارب من القضاء الأمريكي, القدرة على تحدّي القوّة العظمى وإغضابها[٣٥].

ويشكّل ما يسمّى بالإنترنت الخفيّ ***underground internet*** , أو ما يسمّى ب ***Darknet,*** كيانا سيبرانيا آخرا مع بنى تحتية, واقتصاد ونظام مالي, ومساهمين , وزبائن, اذاً قوّة ملحوظة, داخل وخارج الفضاء السيبراني.

ويرى كلّ من ***رولاند, و ريس, و شينوي***, أنّ عصر الكيانات الفضائية, قد بدأ للتو, وهي ستصبح أكثر تطوّرا في المستقبل . فالخيال العلمي, يزخر بقصص تتعلّق بكيانات سيبرانية, كما هو الحال مع السلسلة التلفزيونية ***Matrix.*** ويعتبرون أنّ الكيان السيبراني, قد يكون دولة, أو غير دولة, كشركات, منظمّات إرهابية, أو جمعيات خيرية أو دينية. وهو يعمل ضمن الفضاء السيبراني, كما في العالم المادي, حاشدا موارده من ميادين القوّة الخمسة, للقيام بأنشطة ذات أبعاد متعددة من القوة (الدبلوماسية والمعلوماتية والعسكرية والاقتصادية). وعندهم, إنّ لهذا الكيان إيديولوجية, وجسما سياسيا, وبنية تحتية:

أولاً: إيديولوجية

يستمد الكيان السيبراني إيديولوجيته, والتي هي عبارة عن مجموعة قيم, وأهداف, وسلوكيات,, من العالم المادي. لكن قد يأتي المستقبل, بكيانات سيبرانية, ذات إيديولوجيات, لا علاقة لها بالعالم المادي. ويمكن تصنيف هذه الإيديولوجيات, وفقا لمفاهيم كلّ من الدولة, والشرعية, والدافع الربحي:

أ- الكيان السيبراني بمفهوم "الدولة"

الدول السيبرانية ***cyberstates*** ليست موجودة اليوم, ولكن دولة المستقبل السيبرانية, قد تشبه الدولة, بمفهومها الحالي, بكثير من النواحي. فغالبية النشاطات المتعلّقة بالإتصال بين الدولة ومواطنيها, ستتم من خلال الفضاء السيبراني. ولكن ستبقى الدولة السيبرانية, تعتمد على العالم المادي, بما يتعلّق بوجود الجسم المادي المكوّن لها, والبنى التحتية, والدفاع عن سيادتها في الميادين الخمس.[٣٦] إنّ دولاً كثيرة, تتطوّر, اليوم لتصبح شبيهة أكثر بالدول السيبرانية, من خلال التحوّل نحو حكومات الالكترونية, التي

[35] http://www.reuters.com/article/us-usa-security-snowden-russia-idUSBRE9700N120130801

[36] Rowland & Shenoi, The anatomy of a cyber power, p:4

تستخدم تقنيات الفضاء السيبراني, من أجل تقديم المعلومات والخدمات لمواطنيها. هذه الدول,تعتمد اقتصاديات الكترونية, من أجل خفض معدلات البطالة, وزيادة الناتج القومي[٣٧].

فالفضاء السيبراني, يعطي الدولة القدرة على ممارسة نفوذ دبلوماسي, و معلوماتي, و عسكري, و إقصادي. فهو ميدان جديد من الحروب. والعديد من الدول, يستثمر في المجال التكنولوجي, الذي يمكّنه من إدارة العمليات السيبرانية, لا سيّما العسكرية منها.

أما الكيانات السيبرانية من غير الدول, من شركات, ومجموعات إرهابية, وحركات سياسية ,وإجتماعية, وإقتصادية, ودينية, فإيديولوجيتها متنوّعة, وبعضها متميّز ,عمّا هو موجود في العالم المادي[٣٨].

ب- الشرعية

إنّ الكيانات السيبرانية, كنظيراتها من الكيانات المادية, قد تعمل ضمن القانون, أو خارجه. لكن التشريعات القضائية ,المتعلّقة بالفضاء السيبراني, لا تزال معقّدة لا سيما بما يتعلّق بكيفية تحديد موقع إطلاق النشاطات الإجرامية, وبالتالي الأطر القانونية التي تتناسب معه[٣٩]. وغالباً ما تعمل الدول السيبرانية, والشركات, والحركات السياسية والاجتماعية والدينية, ضمن إطار قانوني محدّد, لكنّ الكيانات الإجرامية, أو تلك التي تعمل في الظلّ, ستستفيد من الفضاء السيبراني, لكسب المزيد من الغموض حول هويتها , ومن السرعة في تحقيق أهدافها, ومن سعة في الانتشار. هذه الكيانات, تشمل المجرم العادي, والمنظمّات الإرهابية, وكذلك منظمات سرية, مثل ***ويكليكس Wikileaks*** , ***وانونيموس Anonymous***, والفئات الهامشية, الباحثة عن اختلاق الفوضى, أو عن المتعة, على سبيل المثال لا الحصر.

ج- الدافع الربحي

إنّ الشركات السيبرانية, والمنظمات الاجرامية, ستعمل في الفضاء السيبراني , كما في عالم الواقع, على تحقيق الربح. أما الكيانات الاخرى , كالمنظمات الغير ربحية مثلا, أو المنظمات الإرهابية, ستستفيد من الفضاء السيبراني, من أجل الترويج لأفكارها, ونشاطاتها . ولكنها, وإن كانت غير ربحية في الأساس, الاّ

---

37 *Bilbao-Osorio, B., Dutta, S., & Lanvin, B. (2013, April). The global information technology report 2013. In World Economic Forum,* p74-60

38 Paganini, P. (2012). The rise of cyber weapons and relative impact on cyberspace. *Infosec Institute, Elmwood Park, Illinois(http://dx. doi. org/resources. infosecinstitute. com/the-rise-of-cyber-weapons-and-relative-impact-on-cyber space*.

39 Menthe, D. C. (1997). Jurisdiction in cyberspace: a theory of international spaces. *Mich. Telecomm. & Tech. L. Rev p:* 70-71

أنّ فرادة الفضاء السيبراني, قد تدفع بها, مستقبلا, نحو تحقيق الربح, من أجل تعزيز اجنداتها العقائدية, ومن أجل ضمن بقائها, ونموها.

ويمكن للإقتصاد السيبراني, أن يشهد تداول ما يسمى ب"النقود الإلكترونية "***cyber cash***", واستخدام بطاقات الائتمان المصرفية, لتبادل السلع والخدمات الالكترونية . مما يعطيه القدرة على مجاراة الإقتصاد في العالم الواقعي, و حيث يساهم إقتصاد الانترنت, في تحويل الأموال, الى أموال سيبرانية, وبالعكس.كما أن الكثير من الألعاب الافتراضية, تسمح للاعبين بالإنخراط في تحويلات, بين العالمين السيبراني والمادي. لكنّ الأدوات والتقنيات المستخدمة في التحويلات, قد لا تكون دائما قانونية. فالاحتيال, وتبييض الأموال, والتهرّب الضريبي, هي من الأمور المألوفة في هذا الفضاء.

لكن المشكلة المتعلقة بالاقتصاد السيبراني, هي أن المستخدمين يمكن أن يكونوا مجهولين, والمعاملات يصعب التحقّق منها . إنّ اقتصادا سيبرانيا شرعيا, لا يمكن أن يزدهر, الاّ في ظلّ تشريعات, تعزّز الثقة بين المستهلك والمنتج في هذا الفضاء .

ثانياً- الجسم السياسي

هو العنصر البشري المكوّن للكيان السيبراني. ويتألّف من الهيئة الادارية, ومن الأفراد "الأعضاء", أي المساهمين, والمناصرين , والمواطنين, والمشاركين العرضيين.

أ- الهيئة الادارية

نتيجة التطوّر المتسارع, لميدان الفضاء السيبراني, ستبرز أشكال جديدة من الكيانات السيبرانية, وستكون القيادة فيها مميزة, مقارنة بما هو موجود في العالم الواقعي,. إن البعض سيفتقد القيادة المنظمة, وسيكون للأفراد الأعضاء, حرية التحكّم في البناء والمضمون . لكن, و ربما مع الوقت سيصبح الفضاء السيبراني أكثر تنظيما .

ب- الأفراد الأعضاء

يمكن ترتيبهم على الشكل الآتي:

- المواطنون وهم أعضاء في الدولة السيبرانية, كما في الدولة الواقعية, وسيعملون بموجب عقد إجتماعي مع الدولة, ضمن هذا الفضاء.
- المساهمون: من شركات إلكترونية, وصناعات, ومنظمات اجرامية ومستثمرين.
- المناصرون: وهم أفراد ينتمون الى مجموعات سياسية, ودينية, واجتماعية, أو حتى ارهابيون.

- المشاركون العرضيون: وهم قلّة, يشبهون المواطن غير المبالي, الذي لا يصوّت, أو صاحب الأسهم القليلة في شركة, والذي لا يتابع تطوّرها, او المسيحي الغير ممارس لطقوسه, او مستخدم الفيسبوك, الذي يراقب فقط, ونادرا ما يشارك .

ثالثاً: البنى التحتية

هي مكوّنات في الفضاء السيبراني, كما في العالم المادي , اللذين يتكاملان, لإظهار نفوذ في الأبعاد الأربعة للقوة:

- بنى تحتية مادية من أجهزة, وبرمجيات, وبيانات, وشبكات ,و مجال مادي للعمل.
- بنى تحتية سيبرانية: وهي الأصول السيبرانية, الغير ملموسة, مثل البرامج, والبيانات المتحركة, وغيرها من العمليات المنفذة عبر الانترنت.[٤٠]

---

[40] Rowland & Shenoi,The anatomy of a cyber power. p:5-6

المبحث الثاني: السيبرانية والعلاقات الدولية: الحاجةُ الى إعادةِ تموضع النظريات التقليدية

حيث إنّ صياغة النظريات بميدانٍ ما, تنطلق من المعطيات المتوافرة, فإنّ تغيّر هذه المعطيات, وبروز وقائع جديدة, من شأنهما الدفاع بشأن إعادة النظر فيها. وهذا ينطبق على النظريات الواقعية, والليبرالية, والبنائية.

فما بين دفاع الواقعيين عن دور الدولة كلاعب أساسيّ في الفضاء السيبراني, وتأكيدهم على أنّ فوضى النظام الدولي ستظلّ قائمة في هذا الفضاء, وتناغم الليبراليين مع السيبرانية, لجهة ما فرضته من تراجع لدور الدولة, لصالح بروز لاعبين جدد في هذا الفضاء, ورؤية البنائيين للفضاء السيبراني كميدان خصب لنشر الرموز والأفكار, تبرز حاجة ماسة الى تحديث نظريات العلاقات الدولية للتلاؤم مع الوضع السيبراني الجديد.

المطلب الأول: الواقعية الجديدة في الفضاء السيبراني بين التأييد والنقد

هناك من يدحض مقولة معظم الليبراليين والبنائيين, بأن الدولة, اليوم, فقدت موقعها المركزي, لصالح الشركات المتعدّدة الجنسيات, واللاعبين من غير الدول, والأفراد, وذلك بسبب تزايد ظاهرة الإعتماد المتبادل عالميا. لا بل يرون أن قوة الدولة, لاسيّما الكبرى, هي في نمو مطّرد. وما الهجمات السيبرانية, التي يشنّها القرصان الفرد, في الفضاء السيبراني, الاّ عمل هواة "***lone wolves***", ولا تشكّل تهديدا للبنى الهيكلية للدولة. فمجموعات مثل ***أنونيموس Anonymous***, يمكنها أن تلحق أضرارا باقتصاد دولة ما, ولكنها لا تعرّض وجود هذه الدولة للخطر. إنّها "بلطجة النظام الدولي الرقمية" ***digital thugs***. و أنّ الجرائم السيبرانية, كالجرائم العادية, مجرد مشاكل عادية تواجهها الدولة, لكنها لا تشكل تهديدا لوجودها, الاّ عندما ترعاه أو تنفّذه, دولة أخرى. فعندها يصبح الوضع تهديدا للأمن القومي للدولة.[٤١]

ويقدّم ***غي غولدستاين Guy Philippe Goldstein***, تعليلات لترجيح الكفة لصالح الدولة في الفضاء السيبراني, ومنها:

[41] Buijs, G. (2012). The Relative Power Of Bits and Bytes,Cybersecurity in power perspective,p:12

- إنّ الدول وحدها قادرة على المواظبة والاستمرارية, في تطوير أسلحة سيبرانية قوية.

- إنّ الدول وحدها قادرة على توظيف المهارات العالية, وتأمين الاستثمارات المالية الضخمة المطلوبة, لعالم تكنولوجيا المعلومات. فـ***رالف لانغنر Ralph Langner,*** والذي يعود اليه الفضل في انهيار دودة ستكسنت ***Stuxnet*** , التي أطلقت على أجهزة الطرد النووية الايرانية, يذهب الى القول, أنه يستحيل على القراصنة الأفراد, أن يخلقوا مثل هذا السلاح المعقّد, لأنه يتطلّب تضافر جهود مهندسين, على درجة عالية من الكفاءة.[٤٢] وينتهي الى القول, إنّ دعم الدول هو أمر مطلوب, من أجل تصنيع أسلحة سيبرانية, معقّدة وخطيرة. وهذا ماتؤكّده شركات أمن الشبكات, مثل ***كاسبرسكي Kaspersky Lab and F-Secure.***[٤٣] وبالتالي, إذا كان لأحد امكانية إحداث ضرر, أو إطلاق تهديد بهذه الدرجة من الخطورة, فهي الدول نفسها.

وهناك من يرى أنّ النظام الدولي قائم على الفوضى, حيث لا وجود لسلطة عليا أو حكومة عالمية. ***فجون مرشماير John Mearsheimer ,*** يقول أنّ الدول لا تستطيع أن تتصل برقم الطوارئ ***٩١١*** عندما تقع بمشاكل, فعليها حلّها بنفسها.[٤٤]وهذا يعني, أنّ أي تصادم بين الدول الكبرى, سيترتّب عليه عواقب وخيمة, لا سيّما بغياب سلطة حيادية للفصل بينها. وهذا ما يشكّل معضلة أمنية, تدفع الدول على التسابق في التسلّح, لتعزيز أمنها, وتفوّقها على الدول الأخرى. وهذا ما يحدث في الفضاء السيبراني,لأن التطوّر التكنولوجي المتسارع, يدفع الدول الى اللحاق بهذا الركب. ويدافع ***ويليام لين William Lynn,*** نائب وزير الدفاع الأمريكي السابق, عن تطوير الولايات المتحدة للقدرات الهجومية, في الفضاء

---

42 Ralph, L,"(December 2011)."Destructive Cyber Weapons https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon?language=en?utm_source=tedcomshare&utm_medium=referral&utm_campaign=tedspread

43 Kaspersky Lab,'Stuxnet Worm:Insight from Kaspersky Lab' http://www.kaspersky.com/au/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm

44 Mearsheimer, J. J. (2001). *The tragedy of great power politics*. WW Norton & Company.p:17 https://samuelbhfauredotcom.files.wordpress.com/2015/10/s2-mearsheimer-2001.pdf

السيبراني, بقوله إنّ أكثر من ثلاثين دولة, أنشأت وحدات سيبرانية في قواتها العسكرية, فمن غير الواقعي الإعتقاد, أن كلّ واحدة منها, ستحدّ من قدراتها الدفاعية.[٤٥]

وبدّد ***كينيث والتز Kenneth Watz*** إدّعاء الليبراليين, أنّ الاعتماد الاقتصادي المتبادل والحالي بين الدول, قد خفّف من آثار الفوضى الدولية. واستبعد اللجوء الى الحرب, معتبرا أنّ ازدياد الاتصال والتفاهم بين الدول, من شأنه ايضا أن يزيد من فرص الصراع بينها.[٤٦] كما أن هناك دولا تستفيد, من الاعتماد المتبادل أكثر من غيرها, ما يخلق اعتمادا متبادلا غير متماثل, يثير امتعاض الدول الأخرى[٤٧].

كما أن ***كلارك***, أيّد الواقعيين, في سخريتهم من تأثير الاعتماد المتبادل, حيث أشار الى أنه, وبسببه, فإن الكمبيوتر الذي يباع في الولايات المتحدة الامريكية, قد تم تصنيع كل أجزائه خارجها, وذلك في دول كالصين, والهند ,ما يعني اختراقا للأجهزة والبرامج, من قبل دول منافسة.[٤٨]

وتتجلّى الفوضى في الفضاء السيبراني, في استهداف القراصنة للكمبيوترات, في أنحاء العالم كافة دون أية مقاومة. فالتشريعات محدودة, والمنظّمات الدولية كالأمم المتحدة, عاجزة عن فرض سلطتها في هذا المجال. ولعل من أبرز أسباب غياب التشريعات, هو أن الإنترنت بنيت على الثقة,حيث لا ضرورة لتكثيف الحماية حول تبادل عدد محدود من المستخدمين للمعلومات بين بعضهم البعض. ولكن مع تزايد الإقبال على استخدام الانترنت, ازدادت الحاجة الى المزيد من الحماية. وقد يكون السبب الآخر, هو أن الدول تستفيد من هذا الوضع, وبالتالي تتردّد حيال تغييره.[٤٩]

أما بالنسبة للأمن القومي, أو بقاء الدولة, التي ينادي بها الواقعيون, والتي يصفها ***مرشايمر*** ب"الهدف الرئيسي للقوى العظمى."[٥٠] فإنّهم يتنبأون, بأنه عندما تجبر دولة على أن تختار بين الثروة والأمن, حكما ستختار الأمن.[٥١]. وفيما يتعلق بالفضاء السيبراني, حيث الأولوية هي للحرية, والخصوصية, والاستقلالية,

---

[45] Lynn III, W. J. (2011). The Pentagon's Cyberstrategy, One Year Later. *Foreign Affairs* https://www.foreignaffairs.com/articles/2011-09-28/pentagons-cyberstrategy-one-year-later (last visited august 3,2016)

[46] *Waltz, K. N. (2000). Structural realism after the Cold War. International security*,,p;14

[47] Ibid p:15

[48] Clarke, R. A., & Knake, R. K. (2011). *Cyber war*. HarperCollins.p:48

[49] Buijs,the relative power,p:15

[50] Mearsheimer, *The tragedy of great power politics*,p:31

[51] Ibid,P:48

يصف مكتب التحقيقات الفدرالية ***FBI***, الثغرات الأمنية للولايات المتحدة في الفضاء السيبراني, بأنها "تهديد وجودي".[52]

ولكن ***عبد الصادق,*** وفي كتابه "الفضاء الالكتروني والعلاقات الدولية", يجادل بأنّ الفضاء السيبراني أثّر على الاتجاه الواقعي في العلاقات الدولية, سواء فيما يتعلق ببعده التقليدي, أو الهيكلي البنيوي, موردا الأسباب التالية :

- أصبحت الدولة تشهد بروز لاعبين جدد في الفضاء الالكتروني, في السياسة المحلية, ما أدى الى الحد من قدرة الدولة على صنع السياسة الخارجية, كتنامي دور الأفراد, واالشركات, والجماعات الارهابية, في استخدام الفضاء السيبراني, إمّا تعبيرا عن مصالحها, أو كوسيلة إعلام دولية الطابع, تعمل على نقل نشاطها المحلي الى السياق العالمي. فالمنظور التهميشي للاعبين من غير الدول, الذي رفعت لواءه المدرسة الواقعية, لم يكن يدرك سوى الدولة كلاعب مهيمن, وأن السياسات الدولية هي كفاح من أجل القوّة. ورغم أن الواقعية الجديدة على يد ***والتز***, سعت الى (إعطاء) دور ثانوي للاعبين من غير الدول, فانها رأت أن هيكل النظام الدولي, يتغيّر فقط بتغيّر توزيع القوّة, والأكثر قوّة هو الذي يعرف بالنظام الدولي, وهو الدولة.
- أثّرت ظاهرة الفضاء الالكتروني على رؤى الاتجاه الواقعي, فيما يتعلّق بمفهوم الدولة القومية, والمصلحة, والردع, والصراع, والحرب. فبينما يركز الاتجاه الواقعي على القوّة العسكرية, من أجل تحقيق الدول لمصالحها, أو الدفاع عنها, برزت أدوات أخرى, كاستخدام القوة الناعمة في تحقيق أهداف السياسة الخارجية للدول, بالإضافة الى دور هذا الفضاء في تحسين وإعادة هيكلة الأجهزة الامنية والاستخباراتية,على نحو أكثر اعتمادا على ثورة المعلومات التي أتاحها. وعلى الرغم من أنّ مفهوم القوّة, ما زال يمثّل أحد مرتكزات تحليل العلاقات الدولية, فإن هذا الفضاء, قد أدّى الى التأثير في طبيعتها, وأنماط استخدامها, وطرق توزيعها بين القوى الرئيسية المشكلّة للنظام الدولي.

---

[52] **Cyberattacks an 'existential threat' to U.S., FBI says**,FBI official warns about increasing cyber–sophistication of rogue states, criminals
http://www.computerworld.com/article/2516690/cybercrime–hacking/cyberattacks–an––existential–threat––to–u–s–––fbi–says.html

- اختلفت طبيعة الصراع, عبر الاتجاه الى الصراع داخل الدول, بدلا من بين الدول في العلاقات الدولية.
- أدّى دور الفضاء الالكتروني في الإندماج والاعتماد المتبادل, الى الحد من قوّة الدول وسيادتها, وهو ما كان له تأثير على فكرة توازن القوى, التي تشكّل جوهر نظرية ***والتز***, بعد التحولات التي أحدثها هذا الفضاء في النظام الدولي, والتي ركّزت على دور المجال الاقتصادي, بدلا من توازن القوى, في المجال العسكري.
- أثّر الفضاء الالكتروني على نمط القوّة في العلاقات الدولية, وذلك من خلال إعادة ترتيب, وتوزيع عناصر القوّة, نجم عنها تراجع للقوة العسكرية, لصالح القوّتين الاقتصادية والتكنولوجية, اللّتين شهدتا حالة من التداخل والتشابك. وعلى الرغم من تناول القوّة كهدف أساسي تسعى اليه الدولة, وفق المدرسة الواقعية, فإنّه تمّ التركيز على بعدها الصلب. وبخاصة أنّ الفضاء الالكتروني, قد عمل على التقليل من أهمية القوّة العسكرية, لصالح قوّة المعرفة والمعلومات, والتي أصبحت محرّكا للقوّة والسيطرة في النظام العالمي .
- على الرغم من أنّ الواقعية, رأت أن التحالفات بين الدول, تزيد من القدرة على ممارسة القوّة, إلاّ أنها لم تدع الى وجود اعتماد متبادل, أو ولاء بين الدول المتحالفة. وهو ربما ما مارسته الولايات المتحدة في التجسّس الالكتروني على حلفائها الأوروبيين, تحت المطالبة بالاستحواذ, والتنافس العالمي على قوة المعلومات والمعرفة.
- أكّدت الواقعية, على أهمية الموقع الجغرافي للدولة, في التعبير عن إمكاناتها وتوجهّاتها في السياسة الخارجية, وعلى تأثير المناخ, على قدرة الدولة على تعبئة قدراتها لمواجهة الدول الأخرى, وهو ما يصطدم بما فرضه الفضاء اللالكتروني, من تحوّل العالم الى قرية صغيرة, ومتجاوزة للحدود. ومن ناحية أخرى, إنّ دخول تكنولوجيا الاتصال والمعلومات في النظم التسلّحية, قد عمل على تقليل أهمية الموقع الجغرافي, كنطاق حامٍ للدولة, مع القدرة على اطلاق الصواريخ العابرة للحدود, وفي السيطرة على الفضاء الخارجي.
- ويعتبر الواقعيون التهديدات الأمنية, ذات الصلة بتكنولوجيا المعلومات في مجملها, بمثابة مشكلة اقتصادية, ولا تؤثر بالضرورة في أمن الدول, ولا تعد في حد ذاتها تهديدات امنية.[٥٣]

---

[53] د.عبد الصادق عادل,الفضاء الالكتروني والعلاقات الدولية: دراسة في النظرية والتطبيق, المكتبة الاكاديمية, الطبعة الأولى, ص:٩٣-٩٩

- اذا, وعلى الرغم من صوابية الواقعية البنيوية أو الجديدة, لجهة القلق من المأزق الأمني السيبراني, الذي يبرز الضعف لديها, في تركيزها على الدولة كمحور اهتمام, وتهميش اللاعبين من غير الدول. فإنّ الحروب التقليدية تديرها الدول,ويصعب على اللاعبين الاخرين حشد جيوش أو قوّة مسلحة كافية, لتقف في وجه قوّة الدول. ففي ساحة المعركة السيبرانية, يمكن لأي كان شن هجوم. وبالرغم من أنه لا يمكن إنكار موارد الدول المالية والتقنية, الاّ أنّ للشركات, والمنظّمات الإرهابية, والأفراد, القدرة على إلحاق الضرر في الفضاء السيبراني. كذلك, إنّ طرح الواقعيين لقدرة الضربة الاولى على انهاء المأزق الأمني, وشلّ قدرات الخصم على الرد, أمر مبالغ به. ففي الحرب السيبرانية, يستحيل تقريبا, أن نرى أو نتوقّع الضربة القادمة. ومع عالمية شبكة الانترنت, لا تستطيع الدول, الحؤول دون شنّ العدو لهجوم مضاد.
- ويركّز كلّ من ***اريكسون وجيوكوملو Eriksson and Giocomello,*** على أن الحكومة وحدها, لا تستطيع أن تجعل الفضاء السيبراني آمنا, ولكنها لا توفر بديلا لذلك.[٥٤]

المطلب الثاني: التناغم بين الليبرالية والسيبرانية

بالنسبة **لليبراليين**, لقد ساهم الفضاء السيبراني, في دعم مقولاتهم, من خلال دوره في خلق تعدّدية في الجهات الفاعلة الدوليّة, وفي العمل على تصاعد دور العوامل السياسيّة, في تحديد طبيعة السياسة الدوليّة, وفي إظهار دور المؤسّسات الدوليّة, في إنشاء, وليس فرض قواعد السلوك للدول, وأدّى الى توسيع أجندة الدراسات الدوليّة, مثل: الأمن السيبراني, والإقتصاد الرقمي, والتنمية. كما أكّد الفضاء السيبراني, على النتائج الإيجابية للإعتماد والترابط المتبادلين, بدلا من التأكيد على إمكانية زيادة سرعة التأثّر, وما يتبعها من إنعدام أمني.

فالليبراليون يرون أن ثورة المعلومات, أعطت القوّة للاعبين من غير الدول. فهي أمّنت الإتّصال العالمي بين المنظّمات غير الحكومية, وغيرها من المجموعات, فكان التأثير الايجابي لذلك واضحا, من خلال التداخل, والتعاون, والتحرّر. لكنّه ايضا أوجد الكثير من السلبيات, ليس أقلّها الإرهاب, والجريمة العابرة

---

54 Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations:(IR) relevant theory?. *International political science review*, *27*(3), p:231 http://www.jstor.org.ezproxy.aub.edu.lb/stable/pdf/20445053.pdf

للحدود, وزعزعة استقرار الدول. من هنا شدّدوا, على أهمية التعدّدية, في المساهمة في ترسيخ الأمن, في العصر الرقمي.[55]

فبالنسبة لهم, إنّ وجود المنظّمات الدولية هو الحلّ, للخروج من هذا المأزق الأمني. وقد يكون من الصعب إنشاء منظمّة دولية, تضم أعضاء من دول وغير دول, مكرسّة أهدافها, ومساعيها, لصيانة الأمن السيبراني, من شأن وجودها أن يخفّف من عامل اللا ثقة, الذي تواجهه الدول. ففي هذه المنظمّة, يكشف الأعضاء عن إمكاناتهم السيبرانية, ويتشاركون التقنية الدفاعية المتطورة لديهم, ما يعزّز الثقة والشفافية في المجتمع الدولي. وبالتالي, إن أي هجوم يقوم به أحد الأعضاء, يمكن تحديده ومعاقبته. أما تلك الهجمات الصادرة عن جهة خارجية, فيمكن التحرّي عنها, ومعالجتها عبر قوّة جماعية, وليس من خلال لاعب بمفرده. ولكن للأسف , يتطلّب ذلك من الأعضاء, الكشف عن معلومات, أحيانا لا يرغبون بنشرها, مخافة إضعاف مركزهم. وهذا ينطبق على القوى العظمى, بالدرجة الأولى, التي قد تتجنّب الإنضمام الى المنظّمة, حتى لا تكون مسؤولة أمامها, عن الأنشطة التي تقوم بها, والمتعلّقة بالحرب السيبرانية.[56]

المطلب الثالث: البنائية: السيبرانية بيئةٌ خصبةٌ لانتشار الأفكار

شدّدت البنائية, على أهمية الرموز والأفكار, ومعانيها. فلقد ركّز اتباعها, على كيفية تغلّب حرب المعلومات, على صعوبات تعدّد الحدود, وبالأخص حدود الهوية , وأن حرب المعلومات هي نوع خاص من حرب الهوية, التي يتم فيها تحدي جميع أنواع الصعوبات الحدودية, ما جعل هويّة حكومة الدولة على حافة الهاوية, على الرغم من بذلها الجهد للتكيّف مع الاختراق الدائم لحدود سيادتها, على نحو رسمي, وبروز هويات جديدة في الفضاء السيبراني.[57]

فبرأي ***موراي ادلمان*** ", إنّ دراسة السياسات الرمزية, ملائمة الى حد كبير لدراسة عصر الأمن الرقمي"[58]. وتصبح عملية استهداف المصالح السيبرانية للدولة, كشن هجمات سيبرانية على مواقعها

---

[55] Ibid,p:235

[56] Petallides, C. J. (2012). "Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat." *Inquiries Journal/Student Pulse*, *4*(03). Retrieved from http://www.inquiriesjournal.com/a?id=627

[57] Ibid

[58] Opcit, p:235

الرسمية, بحسب **عبد الصادق**, "مماثلة لعملية ممارسة التشويه والعدوان, عبر استخدام السياسة الرمزية, وتعتبر أقل عدائية – إن لم تكن مضاهية في درجتها – لحرق علم عدوّ ما, والعمل على فقدان الثقة, والإنتقاص, والإحساس بعدم الأمان عبر الفضاء السيبراني, كالهجمات والهجمات المضادة, عبر مواقع الإنترنت الخاصّة بحكومة الولايات المتحدة والصين,مثلا, من قبل المتسلّلين عبر بلاد مختلفة. ولا تزال هناك حروب سيبرانية مماثلة, بين المتسلّلين الاسرائيليين والعرب, وبين أمثالهما من الباكستانيين والهنود".[٥٩]

ويضيف ***عبد الصادق,*** "إنّ المدرسة البنائية, تقترب من تفسير تأثيرات ظاهرة الفضاء الالكتروني في العلاقات الدولية, عبر إقرارها بعملية التحوّل العالمي في طبيعة المجتمع الدولي, وفي أنّ الدول لم تعد هي اللاعب الرئيسي, وأن المجتمع الدولي كائن يؤثّر ويتأثّر بأجزائه, وهو ما يكشف عن إمكانية المواءمة بين ذلك, وظاهرة الفضاء السيبراني, والتي تجمع مناطق العالم المختلفة, في نظام ومجال الكتروني واحد يخضع لشروط وأحكام تنظيمية واحدة."[٦٠] ويشير ***عبد الصادق*** الى بعدين مهمين للبنائية:

- دور الأفكار والتداخل بين البنية واللاعب في العلاقات الدولية, وهو ما يمكن أن يقدم أطرا تفسيرية للدور الذي يلعبه الفضاء الالكتروني في تصاعد دور الأفكار, والتعبير عن الواقع ذي الطبيعة التفاعلية, والموجود نتيجة التواصل الاجتماعي الذي يسمح بتقاسم بعض المعتقدات والقيم .
- دور الفضاء السيبراني في تصاعد دور الهويات وتأثيرها على سلوك الوحدات ومصالحها, وأصبحت الهويّة والمصلحة تتشكّل عبر عمليات التفاعل عبر ظاهرة الفضاء اللالكتروني, وهو ما يكون له تأثير على سلوك اللاعبين في العلاقات الدولية. ويساعد من ناحية أخرى الفضاء الالكتروني, في الكشف عن هويّات مختلفة للاعبين, وهو ما يعمل على سقوط الفصل بين الداخل والخارج, في دورهما في التأثير على سلوك اللاعبين الدوليين عبر الفضاء السيبراني. وقد أثّر الفضاء الالكتروني في تعزيز النظرة البنيوية في العلاقات الدولية, من خلال دوره في تعدّد اللاعبين في مجال التعبير عن الهوية, وقد أصبحت الهويّة محدّدا بقوّة في عملية صنع السياسة الخارجية, مع تعاظم دور الجماهير في الحشد والاحتجاجات, وعملية التفاعل بين النظم الحاكمة وشعوبها, وفي نفس الوقت أصبح يتم استخدام الهويّة والثقافة, لحشد وتعبئة الجماهير عبر أدوات

---

[59] عبد الصادق,الفضاء الالكتروني والعلاقات الدولية, ص: ١٠٤

[60] م.ن, ص: ١٠٥

الرأي والتعبير عبر الفضاء الا لكتروني, وعبور عملية التعبير عن الهويّة الحدود الدولية, وقيام تحالفات خارجية مستخدمةالفضاء اللالكتروني, في تكوين تكتلات وجماعات ضغط ,تعبّر عن الدفاع عن الهوية وهو ما أدى الى امكانية استخدامها لزعزة استقرار النظم الأخرى في النظام الدول".[٦١]

[61] م.ن,ص:١٠٦

الفصل الثاني: القوة ما قبل الفضاء السيبراني وما بعده

عادة ما تجنّد الدولة قدراتها على تحقيق أهدافها الخارجية من خلال استخدامها لوسائل مختلفة, أهمها الدبلوماسية, الدعاية, الأدوات الاقتصادية. ولكن أصبح من المتعارف عليه في مجال العلاقات الدولية, أنّ مصادر وأشكال القوّة تتغيّر. فاعتبارات عدة تحدّد شكل القوّة, ومن يمتلكها, ومدى تأثيرها في العلاقات الدولية. واليوم, ومع القدرة الهائلة التي أوجدتها ثورة المعلومات في انتاج التكنولوجيا المتطورة, جاء الفضاء السيبراني ليفرز شكلاً جديداً من أشكال القوة. من هنا, أحاول, من خلال هذا الفصل, بعد تعريفي لمفهوم القوة, وتبيان التحوّلات في أشكال القوّة, إبراز تأثير تكنولوجيا المعلومات في خلق ما يسمى بالقوة السيبرانية, ذات المزايا المتعددة, مع الإشكالية التي يطرحها تصنيف هذه القوة الجديدة في ظل الأشكال المتعدّدة للقوّة.

المبحث الأول: التحوّل في القوة: تراجع الصلبة منها لصالح أنماط جديدة

لقد راج في مرحلة معيّنة, مفهوم القوة الذي يركّز على الاعتبارات العسكرية والاقتصادية, ومدى قدرة الدولة على استثمارها لاخضاع الآخرين لرغباتها, تبنّته المدرسة الواقعية, وجرى النظر الى العلاقات الدولية من خلاله. ولاحقاً برز ما يسمّى بالقوّة الناعمة, التي ترتكز على الجاذبية والإقناع. وبدا أن أيّاً من المفهومين, غير قادر على تفسير ما يجري دولياً, بطريقة وافية, فبرز مفهوم القوّة الذكيّة, جامعاً بين الأثنين.

المطلب الأوّل: ماهية القوّة في العلاقات الدولية

"في العلاقات الدولية, إمتلاك "القوّة" يعني إمكانية التأثير على الآخر ليتصرّف بطرق لم يكن ليتصرّف بها, بوسائل أخرى"[٦٢]. ويشبّهها ***ناي*** بالطقس, " الكلّ يتحدّث عنها ولكن قلّة تفهمها. فكما يحاول المزارع

[62] Wilson,E.J.(2008)."Hard power, soft power, smart power." *The Annals of the American Academy of Political and Social Science* 616.1,p:114

والأرصاد الجويّة التنبؤ بالعواصف, كذلك يحاول المحلّلون والقادة السياسيون, فهم ديناميكية التغيّرات الرئيسية, في توزيع القوّة بين الدول"[٦٣].

قديماً, حدّد أرسطو في كتابه "السياسة", القوّة بأنها: "تلك الإمكانية التي تتوفّر لبعض أفراد المجتمع السياسي, لحمل الآخرين على القيام بما لم يكونوا بفاعليه من تلقاء أنفسهم, وحتّى تتضّح فاعلية هذه القوّة, لا بدّ من ممارستها, فيرضخ الآخرون لطلب صاحب القوّة, وينفذّون إرادته"[٦٤].

وعرّف ***توماس هوبز Thomas Hobbes***, في القرن السابع عشر, القوّة بأنها :" الوسيلة المتاحة في وقت معيّن, للحصول على خير مستقبلي واضح"[٦٥]. أما بالنسبة ***لماكس ويبر Max Weber***, فالقوّة هي لعبة, حيث المجموع الصفري, هو محصلّتها النهائية, فإما أن تفوز أو تخسر. وهي "إحتمال قيام شخص ما في العلاقات الاجتماعية بتنفيذ رغباته رغم مقاومة الآخرين, بغضّ النظر عن الأساس الذي يقوم عليه, ذلك الاحتمال".[٦٦]

كذلك عرّفها ***بلو P. M .Blau*** بأنّها " قدرة الأشخاص او المجموعات على فرض إرادتهم على الآخرين, رغم مقاومتهم لذلك, من خلال الأساليب الزجرية, كإيقاف التمويل المادي أو فرض عقوبات سلبية معيّنة"[٦٧]. ويبرز من خلال هذا التعريف, العنف كعنصر أساسيّ في علاقات القوة, على الأقل عند انعدام التوافق. فالقوّة ليست استعراضا فعليا للتفوّق, إنما هي أرجحية حاضرة دائما.

وعرّفها ***هانز مورجنثاو Hans Morgenthau*** بأنّها :" القدرة على التحكّم في أفكار وأفعال الاخرين."[٦٨] في إشارة واضحة الى عنصري القوّة الرئيسيين, وهما: الإمكانيات والفعل.

أمّا ***روبرت دال Robert Dahl***, فقد عرّفها بأنّها إمكانية "أ" على حمل "ب" للقيام بما لن يقوم به".[٦٩]

واعتبر كلّ من ***ميشال بارنيت وريمون دوفال Barnett and Duvall*** أنّ هذا التعريف, من حيث

---

[63] *Nye, J. S. (1990). The changing nature of world power. Political Science Quarterly, 105(2),p:*177-178. doi:1. Retrieved from http://www.jstor.org/stable/2151022 doi:1

[64] عبد القادر احمد علي,د.كمال المنوفي – النظريات والنظم السياسية – ص ٢٠- الطبعة الاولى يناير ٢٠٠٢

[65] خالد الحراري- مفهوم القوة في السياسة الدولية – دار المستقبل – ٢٠١٥ ص:١٢

[66] Pallaver, M. (2011). *Power and its forms: hard, soft, smart* (Doctoral dissertation, London School of Economics).p:32-33

[67] Ibid,p:34

[68] فاروق يوسف. القوة السياسية. القاهرة.مكتبة عين شمس ١٩٨٤ ص ٧

[69] Dahl, R. A. (1957). The concept of power. *Behavioral science*, *2*(3), p.202-203

ناحية السلطة والتأثير, هو الأكثر استخداما, من قبل أكاديميي العلاقات الدولية. فالقوّة بالنسبة ***لدال*** لديها مظاهر ثلاثة:

- تعمّد "أ" تغيير أفعال "ب" في اتجاه معيّن, حيث لا يعدّ تغيير "ب" لأفعاله ممارسة لأية قوّة, اذا كان ذلك مبنيّا على انطباع خاطئ من "ب", بأنّ هذا ما يريده منه "أ", وذلك لغياب عنصر النيّة, من قبل هذا الأخير.
- وجود رغبات متعارضة, الى الحد الذي يشعر به "ب", أنّه مجبر لتغيير أفعاله.
- اعتبار أنّ نجاح "أ", يكمن في قدرته على التصرّف بالموارد المادية والفكرية التي يمتلكها, والتي ستقود "ب" لتغيير أفعاله.[٧٠]

من ناحيتهما, قدّم كلّ من ***بارنيت ودوفال,*** أربعة تصنيفات للقوة[٧١]:

أولاً: القوّة الإلزامية

هي تبرز كلما كانت تصرّفات "أ" تسيطر على سلوكيات "ب", حتى لو لم تكن هذه التصرّفات متعمّدة من قبل "أ" . وهذا رأي كلّ ***من بيتر باشاراك ومارتون باراتز Peter Bachrach and Morton S. Baratz***, والقوّة تظلّ موجودة, حتى ولو لم يكن ممارسوها مدركين للنتائج الناجمة عن ممارستهم لها.[٧٢] واعتبر كلّ من ***بارنيت ودوفال,*** أن القوّة الإلزامية, تمارس من قبل فاعلين من دول أو غير دول, كقدرة الشركات المتعدّدة الجنسيات, على استخدام سيطرتها على رؤوس الأموال, لتشكيل اقتصاديات الدول, أو قدرة المجموعات والشبكات الارهابية, على تخويف الشعوب. كما اعتبرا أنّ القوّة الإلزامية, لا تحتاج أحيانا الى مصادر مادية, بل يمكن أن تنطوي على قواعد ومبادئ معيّنة أيضا. فالدول الأقل نفوذا في منظمّة الأمم المتحدة, قد تلجأ الى القوانين الدولية, من أجل تقييد تصرّفات الدول الأقوى.[٧٣]

---

70 Ibid, p:205

71 van Haaster, J. (2016, May). Assessing cyber power. In *Cyber Conflict (CyCon), 2016 8th International Conference on* (pp. 7-21). IEEE.

72 Bachrach, P., & Baratz, M. S. (1994). Decisions and nondecisions: an analytical framework. *Power: Critical Concepts*, *2*, 95-110

73 Barnett, M., & Duvall, R. (2005). Power in international politics. *International organization*, *59*(01), p;50. Retrieved from http://www.jstor.org/stable/3877878

ثانياً: القوّة المؤسساتية

حيث يسيطر الفاعلون على الآخرين بطريقة غير مباشرة, فقد لا يمتلك "أ" المؤسسات التي تؤثّر وتسيطر على "ب", ولكن هذه المؤسّسات, تكون خاضعة كلّيا لسيطرة "أ".

ثالثاً: القوّة الهيكلية

هي تعنى في تحديد قدرات ومصالح الفاعلين اجتماعيا, بناء على الموقع الفوقي أو الدوني الذي يشغله أحدهم بالنسبة للأخر. وهذا ما عبّر عنه ***ستيفان لوكاس, Steven Lukes***, بقوله:" هي ممارسة القوّة الى الحدود القصوى من الاحتيال",[٧٤] من أجل السماح للاعبين, أو منعهم من الصعود في المجتمعات. وهي تنجم عن جملة إجراءات, ومعارف, وممارسات إجتماعية, تعطي تصنيفات معيّنة مثل: " الدول الديمقراطية",أو"الدول المتطوّرة", أو "الدول المارقة"....[٧٥]

وفي التسعينيات, ميّز ***ناي*** بين القوّة الصلبة والقوّة الناعمة, بحيث تعتمد الأولى على الإكراه والعقوبات, بينما تعتمد الثانية على عاملي الجذب والإقناع[٧٦]. واعتبر أنّه "ليس هناك من تعريف واحد لمفهوم "القوّة", مقبولا من جميع اللّذين يستخدمون هذه العبارة , واختيار الناس لتعريف معيّن, إنما يعكس إهتماماتهم وقيمهم".[٧٧] وعلّق على تعريف ***دال*** للقوّة, بأنّها "القدرة على حمل الآخرين على القيام بما لا ينوون القيام به",[٧٨] بأنّه عندما نقيس القوّة وفقا لتغيّر سلوك الآخرين, علينا أن نعرف تفضيلاتهم, وكذلك تصرّفاتهم, عندما لا تمارس عليهم القوّة . ومن هنا, فإنّ هذا التعريف, بالنسبة للقادة والسياسيين, مؤقّت ولا يصمد طويلا, لأنّ إمكانية السيطرة على الآخرين, غالبا ما تترافق مع إمتلاك موارد معيّنة. فالقادة السياسيون

---

[74] Digeser, P. (1992). The fourth face of power. *The Journal of Politics*, *54*(4),p:979. Retrieved from http://www.jstor.org/stable/2132105

[75] Barnett & Duvall, Power in International Politics,p;56.

[76] Nye, J. S. (2004). *Soft power: The means to success in world politics*. PublicAffairs. http://belfercenter.hks.harvard.edu/files/joe_nye_wielding_soft_power.pdf Published by: Washingtonpost.Newsweek Interactive, LLC Stable URL:http://www.jstor.org/stable/1148580

[77] Nye, *Cyber power*,p.6

[78] Dahl, R. A. (2005). *Who governs?: Democracy and power in an American city*. Yale University Press.

غالبا ما يعرّفون القوّة, بأنّها امتلاك لموارد معيّنة طبيعية, وسكّانية, وجغرافية, وأمنية, وإقتصادية, ما يجعل مفهوم القوّة يبدو ملموسا أكثر, متوقّعا, وقابلا للقياس, أكثر من التعريف المتعلّق بالسلوك.

ولكنّ المشكلة الأساسية التي تبرز, عندما نفكّر بمفهوم القوّة من الجانب المتعلّق بالموارد, إنّما تكمن في تحويل القوة **power conversion** . فبعض الدول أفضل من غيرها, من حيث إمكانية تحويل الموارد التي يمتلكونها, الى نفوذ فاعل ومؤثّر. من هنا, إنّ تحويل القوة هو إمكانية تحويل القوّة الناجمة عن إمتلاك الموارد, الى قوّة ملحوظة وفعلية . أما المشكلة الأخرى, فهي تحديد أية موارد تشكّل أكثر من غيرها, مصدراً للقوّة . ففي المجتمعات الزراعية الأوروبية, في القرن الثامن عشر, شكّل عنصر السكان, كونه مصدراً لليد العاملة وللضرائب, مورداً هاماً للقوّة, وبه استطاعت فرنسا أن تسيطر على غرب أوروبا. كذلك شكّلت الثورة الصناعية, وتطوّر شبكة السكك الحديدية, في القرن التاسع عشر, مصدراً للقوّة. فاستخدام المانيا للسكك الحديدية, لنقل الأسلحة, سرّع في تحقيق الانتصارات. كما أنّ روسيا ,فشلت في تجنيد العنصر السكّاني الكبير الذي تمتلكه, في ذلك الوقت, مقارنةً مع باقي أوروبا. [٧٩]

ويقول ***مرشايمر,*** "فكما المال بالنسبة للاقتصاد, كذلك القوّة بالنسبة للعلاقات الدولية".[٨٠] وعرّف القوة, بأنها "ليست أكثر من الأصول, والموارد المادية التي تتوافر لدى الدولة".[٨١] لكنّ الموارد لا تشكل دائما العنصر الحاسم في النزاعات بين الدول, ففي الحرب الفيتنامية (١٩٥٥-١٩٧٥), مثلا, ورغم أنّ الولايات المتحدة الأمريكية, أضعفت قوّة فيتنام الشمالية البشرية والعسكرية, الاّ أنها لم تستطع أن تمنعها من تشكيل مقاومة, نجحت في كسب الحرب.

أمّا ***جيفري هارت Jeffrey A. Hart*** فقدّم ثلاث مقاربات لملاحظة وقياس القوّة;[٨٢]

- القوّة كقدرة للسيطرة على الموارد.
- القوّة كقدرة للسيطرة على اللاعبين.

[79] Nye, The Changing Nature of World Power. Retrieved from http://www.jstor.org/stable/2151022 doi:1

[80] Mearsheimer, J. J. (2001). *The tragedy of great power politics*. WW Norton & Company.p:7 https://samuelbhfauredotcom.files.wordpress.com/2015/10/s2-mearsheimer-2001.pdf

[81] Ibid,p;57

[82] Hart, J. (1976). Three approaches to the measurement of power in international relations. *International Organization*,30(2), 290-295. Retrieved from http://www.jstor.org/stable/2706260

- القوّة كقدرة للسيطرة على الأحداث والنتائج.

ويرى في هذه الاخيرة ,المقاربة الوحيدة التي تأخذ بالحسبان, الإعتماد المتبادل, والعمل الجماعي بين الدول. ***وكان جيمس كولمان*** ,أوّل من تحدّث عن هذه المقاربة, في كتابه ***the mathematics of collective action*** , وبنى هذه النظرية, على أساس أنّ الأسباب الكامنة وراء التحكّم بالموارد والفواعل, تنبع من الرغبة في تحقيق نتائج معينة. فبدلا من أن يصنع علاقة بين الفواعل والنتائج, قام كولمان, بإعطاء حلقة وسط بين الاثنين, بحيث أنّ كلّ حدث متعلّق, على الأقل, بواحد من النتائج لكلّ فاعل.[٨٣]

نستخلص مما تقدّم, أنّ إيجاد تعريف موحّد للقوة في العلاقات الدولية, أمر معقّد, فليس هناك من إتفاق حول ذلك. ولعلّ تعريف ***هارت*** للقوة بأنها "السيطرة على الأحداث والنتائج"[٨٤], هو التعريف الأفضل, لأنّه لا يأخذ بالاعتبار فقط, إمكانية اللاعب "أ" أن يجعل اللاعب "ب" يقوم بالعمل المطلوب, بل ايضا امكانية "أ", أن يتأكد أنّ اللاعب "ب", لن يقوم بأخذ المبادرة بالقيام بالفعل, حين لا يرغب "أ" بذلك. فهو يأخذ بعين الإعتبار ليس فقط امتلاك الدولة للموارد كمصدر للقوّة, بل أيضا ما اذا كان استخدام هذه الموارد سيفضي الى النتائج المرجوّة. وهذا ما ينطبق أكثر على ميدان الفضاء السيبراني موضوع البحث, لأن الحرب السيبرانية, غالبا ما تصنّف بأنها غير متماثلة, يعني تكلفة قليلة, وموارد أقل, ولكن دمارا هائلا.

المطلب الثاني: أشكال القوّة: بين صلبة, وناعمة, وذكيّة

فقرة أولى: القوّة الصلبة

القوّة الصلبة هي أبسط وأقدم أشكال القوّة, كونها ملموسة وأكثر عملانية, كما أن ممارستها أسهل من القوّة الناعمة,الى حدّ ما. تاريخيا, كانت القوّة تتركّز على "القوّة الحربية", إضافة لعناصر: السكان, والأرض, والموارد الطبيعية, والاستقرار السياسي. فاذا كان للدولة أسطول بحري قويّ, وجيش مدرّب, ورأسمال اقتصادي وسكاني هام, كان بإمكانها أن تلزم الدول المجاورة لها, بالقوّة اوبالرشوة, العمل بما يتماشى مع

---

83 Ibid, p:296

84 Ibid,p:269

مصالحها, وأهدافها. وهذا ما دفع هذه الدول, الى زيادة قدراتها العسكريّة ,لإقامة التوازن مع الدول القويّة, وللوقوف في وجهها. فامتلاك مصادر القوّة, خلق الخوف, وهيّأ للمواجهة, في الوقت نفسه.

يقول ***مورجنثو Morganthau*** : "إنّ القوة العسكرية في السياسة الدولية, هي العنصر المادي الأكثر أهمية, لصنع قوّة الدولة السياسية". وبرأيه, على الرغم من أهمية وجود عناصر أخرى هامّة, وطالما أنّ الدول هي في حالة من الفوضى, فالقوّة العسكريّة ستستمر في لعب هذا الدور الهام, في السياسة الدولية.[٨٥] وهذا ما أشار اليه ***ناي*** بقوله: إنّ النظام العالمي يفرض الحفاظ على هذه القوّة, في ظلّ الفوضى, وغياب حكومة عالميّة لحلّ النزاعات . فبالرغم من أنّ استخدام المباشر للقوة, محظور بين الدول, فإنّ القوّة العسكريّة, تظلّ تلعب دورا سياسيا كمصدر للنفوذ, للوصول الى مصادر الطاقة, أو للتفاوض من أجل الحصول على مكاسب, او لدرء التهديدات. [٨٦]

ويرى ***والتز,*** أنّ الدولة تلجأ الى استخدام القوّة الصلبة إمّا للردع ,او للدفاع, او لإجبار الدولة على تغيير سلوك معين.[٨٧] كما يؤكّد على أنّ " فاعلية القوّة الصلبة لا تزال صامدة , لأنّه في عالم الفوضى, القوّة والسياسة متصلتان, والقوّة العسكريّة وحدها, لا تضمن البقاء أو الإزدهار, ولكنّها دائما المكوّن الأساسي لهما, لأنّ اللجؤ الى القوّة, هو الورقة الاخيرة لكلّ الدول. والنوايا الجديّة للدولة, تنعكس في امتلاكها مركزا عسكريا, له وزن وأهميّة, وعدم وجود ذلك, ينتقص من فاعلية دبلوماسيتها".[٨٨]

ويرى ***أرنست ويلسون,*** إنّ القوة الصلبة المتجذرّة في النيوليبيرالية, تركّز على التدخّل العسكري , والدبلوماسية القسرية, والعقوبات الاقتصادية". ومن مصادر القوّة الصلبة, حاملات الطائرات, والدبابات, والقذائف.... كذلك القوّة الإقتصادية, لسحق إقتصاد دولة أخرى, أو السيطرة على أسواقها. كما أنّ القوّة الصلبة, قد تكون نتاجا للقوّة الإقتصادية, التي تترجم بقوّة عسكريّة. ففي الحرب العالمية الثانية,مثلا, كان للتحالفات العسكريّة, كما للقوّة الاقتصادية, دور هام في القضاء على دول المحور. [٨٩]

---

[85]Troxell, J. F. (2012). Military power and the use of force. *US Army War College Guide to National Security Policy and Strategy*,p: 224-225

[86] Nye, The Changing Nature of World Power

[87] Art, R. J. (2013). *A grand strategy for America*. Cornell University Press. Available from: eBook Collection (EBSCOhost), Ipswich, MA.

[88] Art, R. J. (1980). To what ends military power?. *International Security*, *4*(4),p:35

[89] Wilson, Hard Power, Soft Power, Smart Power,p: 114

ومفهوم القوّة الصلبة, مألوف من الجميع, ويعتمد على الإغراءات (الجزرة), أو التهديدات (العصا), كما يقول *ناي*.[٩٠] وتتعدّد مستويات التهديدات والإغراءات, فلا يكفي التهديد باستخدام القوّة الصلبة, إنما ينبغي (توافر)القدرة على تنفيذ هذا التهديد, فالخداع غير مسموح هنا. أمّا الإغراءات, فمن الوجهة السلبية, تتعلّق بالتفوّق الإقتصادي لدولة ما, على دولة أخرى, وقدرتها على فرض عقوبات إقتصادية عليها. أمّا الوجه الايجابي, فهو عبر حمل دولة ما, على القيام بما تريده دولة أخرى, عبر إغرائها بالمال. فقوّة الدولة الأولى, تنبع من قدرتها على شراء الدولة الأخرى, لكنّ البعض يرى في ذلك مكافأة وليس رشوة, بحيث إنّ الدولة الأخيرة, تكون مستعدة لاتّباع تعليمات الأولى, طالما أنّها ستحصل على جائزة.

اما الإكراه, فله علاقة بإستخدام العنف, وتحديدا المادي منه.فمثلا, إذا توقّفت دولة ما, عن طاعة الدولة المسيطرة, فلهذه الاخيرة خيار آخر, لإقناعها بضرورة الطاعة, عبر إكراهها على ذلك. فالقوّة الصلبة تعتمد على مصدرين أساسيين : المال ووسائل الاكراه.[٩١]

وللحصول على التأثير المطلوب, يجب أن ينظر الى القوّة, وفقا للسياق الذي تستخدم فيه. فالقوّة لا تعتمد فقط على المصادر, بل على طبيعة العلاقة التفاعلية بين صاحب النفوذ, وبين الهدف ودوافع هذه العلاقة. ففي بعض القضايا, إنّ مصادر القوّة, لا تستطيع وحدها, أن تحقّق الأهداف المرجوّة. وفي قضايا أخرى ,تحدث عواقب غير متوخّاة. وقد يكفي أحيانا, استخدام مصدر واحد ليعطي النتيجة المطلوبة, ولكن بتكلفة أعلى بكثير. وقد يكون سبب ذلك, بكل بساطة, نتاجا لقرار الآخر بعدم الخضوع, وبالتالي اختياره للمقاومة. من هنا, لا بد من الآخذ بعين الإعتبار, أنواعا أخرى من القوّة, ومصادر أخرى, يمكن استخدامها لتحقيق أهداف الدولة.[٩٢]

وفي العلاقات الدولية, ترتبط القوّة الصلبة أكثر, بالنظرية الواقعية . فالواقعيون يلاحظون الفوضى في المجتمع الدولي, ويعتبرون أنّ كل دولة تسعى الى زيادة أمنها, عبر الإعتماد على ذاتها فقط, ولا تعطي أي اعتبار لسلطة اخرى تعلوها ,كالمنظمات الدولية, أو القانون الدولي. من هنا, فان هذه النزعة للبقاء,

[90] Nye, J. S. (2004). *Soft power: The means to success in world politics*. PublicAffairs.

[91] Pallaver, M. (2011). *Power and its forms: hard, soft, smart* (Doctoral dissertation, London School of Economics)

[92] Hackbarth, J. R. (2008). *Soft power and smart power in Africa*. Naval Postgraduate School Monterey CA Center for Contemporary Conflict

هي العامل الاساسي الذي يحرّك سلوك هذه الدول, من حيث تطوير قدراتها العسكريّة الهجوميّة, تجاه التدخّل الخارجيّ .

كما أنّ مناصري القوّة الصلبة, لا يعيرون القوّة الناعمة أي اهتمام , كما أنّهم لا يعتبرونها شكلا من أشكال القوّة. مثالا على ذلك, ***روبرت كاغان Robert Kagan*** , في كتابه "الجنّة والقوّة", حيث قال: "إنّ الدول التي تمتلك قوّة عسكريّة أكبر, تعتبر أن القوّة هي الوسيلة الأفضل في العلاقات الدولية, مقارنة مع الدول ذات القدرة العسكريّة الضعيفة. فعندما تمتلك مطرقة, كلّ المشاكل تبدو كأنّها مسامير". ومن هنا, فإن الدول ذات الإمكانيات العسكريّة المحدودة, هي التي ستواجه الخطر المضاد, "عندما لا تمتلك المطرقة لا تريد أن تبدو كمسمار".[٩٣] وبرأيه, إنّ الدول,اذا أرادت أن تحيا في الجنّة, عليها أن تتخلّى عن التعامل بأسلوب القوّة, لأنّ هذه الاخيرة هي "سيئة ووسخة". فالقوّة بالنسبة ***لكاغان***, لا علاقة لها بالجنّة, فهي تعني العنف, وهذا يتنافى مع مفهوم الجنّة. كما عرّف القوّة, بأنّها "القدرة والإمكانية على حلّ المشاكل, عبر استخدام العنف وتوظيف القوّة من خلال خيار الحرب. هذه هي القوّة ,لا أكثر ولا أقل, هي قاسية بلا رحمة, أو شفقة".[٩٤] ***وكاغان*** مثل غيره من الواقعيين, لا يرى أنّ التعبير عن القوّة , يمكن أن يتم بأشكال أخرى, وإذا وجدت, فهي غير فاعلة ولا تأثير يذكر لها.

وتذهب ***دافيس كروس Davis Cross***,[٩٥] الى القول, أنه يجب التمييز بين امتلاك مصادر القوّة, وبين ممارستها كأدة للتأثير, بحيث تعتبرها, في هذه الحالة, وسيلة إكراه فقط, والاّ, فإنّ هذه المصادر نفسها, يمكن ان تستخدم للجذب, أو للإستمالة. فالمصادر التي يعتبرها الواقعيون الجدد أساس القوّة الصلبة, كحجم السكان, والأرض, والموارد الطبيعية, والقدرة العسكرية, والاستقرار السياسي",[٩٦] هي ليست بالضرورة وسائل إكراه, إن لم تستخدمها الدول, من أجل غاية معيّنة. فحقيقة أنه من المتوقّع أن تتخطّى الهند الصين بعدد السكان في عام ٢٠٢٦ , لا يشكّل للكثيرين مصدرا للتهديد. كما أن جهود الإتحاد

---

93 Kagan, R. (2003). Of Paradise and Power: Europe and America In The New World Order. *London: Atlantic.*p:27-28

94 Ibid p:29

95 Cross, M. A. K. D. (2011). Europe as a Smart Power: The Impact of the European External Action Service, APSA 2011 Annual Meeting Paper. Available at SSRN: http://ssrn.com/abstract=1900094

96 Waltz, K. (1979). Theory of international relations. *Reading, Mass.: Addison-Webley*, 111-114

الأوروبي, لبناء قدرة عسكرية مشتركة لا ينظر اليها على أنها نوع من الهيمنة, رغم أن الموازنة العسكرية للدول الأعضاء فيه, تتصدّر المراتب العشر الاولى بعد الولايات المتحدة الاميركية. كما أن القوّة الإقتصادية لليابان, لا تعتبر مصدرا للتهديد, رغم أنها توازي تقريبا القوة الاقتصادية للصين, أوهي بحجم الدين الأميركي. وامتلاك فرنسا للسلاح النووي, لا يمثّل الخطورة نفسها, التي يشكّلها امتلاكه من قبل باكستان, أو الصين.

ورغم أن الواقعيين الجدد يرون أن الزيادة في القوّة العسكرية, كافية لخلق الخوف لدى الدول الأخرى على أمنها. وبالتالي, قادرة على إطلاق شرارة سباق التسلح. فإنّ مضاعفة الولايات المتحدة الاميركية, مثلا, للإنفاق العسكري منذ احداث ١١ ايلول٢٠٠٠, من دون بروز أي تحدّ من قبل دولة أخرى, لمواجهة تفوّقها العسكري, لم يمنعها من خسارة الموقع الآحادي العالمي, الذي كانت تشغله. ومردّ ذلك, عدم قدرتها على تحويل هذا المصدر العسكري, الى قوّة صلبة, في ضوء التحديات التي تواجهها, او لأن استخدامها للقوة العسكرية في العراق, وافغانستان, قد أضعف من موقعها كقوة عسكرية كبرى, وبرهن للعالم, أنّ القوّة العسكرية, قد لا تتمكّن من تحقيق الهدف, الذي استخدمت من اجله.[٩٧]

ولكن, بالرغم من أهمية القوّة العسكرية, الاّ أنّ العديد من الباحثين, أشاروا الى تراجعها, كأداة من أدوات القوّة, في النظام الدوليّ, لأسباب عدّة, جعلت إمكانية اللجوء الى الحرب, أمراً مستبعداَ, حتّى عند أكثر الدول تقدّما.[٩٨] وكما يقول دبلوماسي بريطاني: "إنّ عددا كبيرا من أكثر الدول قوّة, لايريد أن يقاتل أو يغزو".[٩٩]

هذا وعرض ***ناي*** , عام ١٩٩٠, خمسة اتجاهات, أدّت الى انتشار مصادر القوّة في العالم[١٠٠] :

- السلاح النووي, حيث ثبت أن امتلاكه هو امتلاك الدولة "لعضلات مفتولة", وعواقب استخدامه وخيمة ومدمّرة, وأنه خلق توازنا عالميا للقوى .
- تصاعد النزعة القومية. فمن الصعب على الامبراطوريات, أن تحكم الشعوب الواعية اليوم. ففي القرن التاسع عشر , إحتلّ بعض المغامرين, وبعدد قليل من الجنود, معظم قارة افريقيا. وبريطانيا

---

[97] Ibid,p:23-25

[98] Nye, J. S. (2002). Why military power is no longer enough. *The Observer*, *31*, 2002. https://www.theguardian.com/world/2002/mar/31/1

[99] Cooper, R. (2002). The new liberal imperialism. *The Observer*, *7*(02) https://www.theguardian.com/world/2002/apr/07/1

[100] Nye, J. S. (1990). Soft power. *Foreign policy*, (80), 153-171

حكمت الهند بقوة استعمارية, كانت تشكّل نسبة ضئيلة جدا, مقارنة مع عدد السكان الأصليين.[١٠١] أمّا اليوم, فقد واجهت الولايات المتحدة الاميركية, صعوبة في قمع العشائر الصومالية, أو في تهدئة العراق , بالقوّة العسكرية الكبرى التي تمتلكها.[١٠٢]

- الإعتماد الإقتصادي المتبادل, الذي قلّص من إمكانية استخدام القوّة, لأن ذلك يعرّض النمو الإقتصادي, والمصالح المالية, للخطر. حتى الدول الغير ديمقراطية ,التي لا تعير الأخلاقيات في استخدام القوّة أي اهتمام, تأخذ بعين الإعتبار, انعكسات إستخدامها للقوّة, على مصالحها الإقتصادية. وكما يقول ***توماس فريدمان*** ," في ظلّ العولمة, تؤدّب الدول من قبل "قطيع الكتروني" من المستثمرين, الذين يسيطرون على رؤوس الأموال ".[١٠٣]
- اللاعبون العبر_ وطنيون , والشركات المتعدّدة الجنسيات, والمنظّمّات الغير حكومية, وحتى المجموعات الإرهابية, قادرة على ممارسة القوّة, التي كانت سابقاً حكراً على الدولة فقط.
- التحدّيات الأمنية العابرة للحدود. كالإرهاب, والتغيرات المناخية, والقضايا الصحيّة, والإتجار بالمخدّرات, والتي قلّصت من قدرة استخدام القوّة الصلبة في معالجتها. ورغم أن للقوّة دورا هاما أحيانا, لكن أدوات القوّة التقليدية غير كافية للتعامل مع هذه المعضلات العالمية. [١٠٤]

وأضاف ***ناي***, فيما بعد, القوة السيبرانية كإتجاه سادس, ساهم في الإضعاف من فاعلية القوّة الصلبة. حيث إن " المعلومات قوّة, واليوم عدد أكبر من سكّان العالم لديه إمكانية الحصول عليها". وبالتالي, إن ازدياد الديمقراطيات في العالم يجعل التأثير على الشعوب ضئيلا. فالولايات المتحدة, فشلت في الحصول على دعم تركيا, لتمركز قواعدها العسكرية هناك من أجل اجتياح العراق, أو كسب تصويت المكسيك في الأمم المتحدة, للغرض عينه.[١٠٥]

---

101 Nye, J. S. (2002). Limits of American power. *Political Science Quarterly, 117*(4),p:549.

102 Hackbarth, J. R. (2008). *Soft power and smart power in Africa*. Naval Postgraduate School Monterey CA Center for Contemporary Conflict.

103 Friedman, T. L. (2000). *The Lexus and the olive tree: Understanding globalization*. Macmillan.p:107

104 Nye, "Soft Power,"p:157

105 Nye, J. (2008). Public Diplomacy and Soft Power. *The Annals of the American Academy of Political and Social Science, 616*,p:99 . Retrieved from http://www.jstor.org/stable/25097996

وأبرز ***ولسون*** عاملا آخر, هو " التحوّل من الإقتصاديات الصناعية الى ما بعد الصناعية, حيث القوّة باعتماد متزايد على القدرة الوطنية, للتعامل مع المعرفة, والمعلومات وإنتاجها.[١٠٦]

وعلى عكس مناصري القوّة الصلبة, فمناصرو القوّة الناعمة يعترفون بالقوّة الصلبة, ولكنهم يقولون بوجود بدائل, وهي القوّة الناعمة. فما هي هذه القوّة؟

فقرة ثانية: القوّة الناعمة

يبدو مصطلح القوة الناعمة , للوهلة الأولى, بسيطا, فهو عادة ما يعرّف, كنقيض للقوّة الصلبة المتمثّلة بالإكراه. وتعود أصوله الى ***ناي*** , لكنّه ليس أول القائلين, بأنّ القوّة يمكن ممارستها بدون أساليب التهديد أو الإغراء, فمفكّرون أمثال ***فوكالت, Foucault , وبورديو Bourdieu , وغرامشي Gramsci***, وغيرهم, طرحوا أفكارا مشابهة.[١٠٧] حتّى أنّ ***ستيفن لوكس Steven Lukes*** , والذي لا يقلّ أهمية عن هؤلاء المفكرين, ذكر أنّ القوّة يمكن أن تكون فاعلة باتباع طرق تؤثّر لا شعوريا في تكوين تفضيلات الاشخاص.[١٠٨]

لقد قدّم ***ناي*** مصطلح القوّة الناعمة في التسعينيات, [١٠٩] وهدف من خلاله, الى إظهار عدم تراجع قوّة الولايات المتحدة الاميركية في ذلك الوقت, وأنّها, بنظره, ستستعيد موقعها كقوة عظمى رائدة, من خلال اتباع سياسة خارجية, تستخدم القوّة الناعمة. وأصرّ ***ناي*** على أهمية القوة الناعمة للدول, في الحقبة التي تلت الحرب الباردة, لكسب الشرعية, ولإقامة التحالفات, دون الخضوع لتأثيرات الاخرين, وللحؤول دون وقوع مواجهات عسكرية.

---

106 Wilson,"Hard power, soft power, smart power",p:112

107 Mattern, J. B. (2005). WhySoft Power'Isn't So Soft: Representational Force and the Sociolinguistic Construction of Attraction in World Politics. *Millennium-Journal of International Studies*, *33*(3), 583-612. Gramsci, A. (1971). The philosophy of praxis. *Selections from the prison notebooks of Antonio Gramsci*.

108 Lorenzi, M. (2006). Power: a radical view by Steven Lukes. *Crossroads*, *6*(2), p:95

109 In 1990, Joseph Nye introduced the concept of soft power in the book *Bound to Lead: The Changing Nature of American Power* (Nye 1990a), and in an article published in the same year in the journal *Foreign Policy* (Nye 1990b)

ثم أوضح نظريته أكثر فيما بعد,[110] عبر تحليل معمّق لثلاثة مصادر لهذه القوّة الناعمة:

- الثقافة التي تشكّل عامل جذب للآخرين.
- القيم السياسية التي تؤمن بها الدولة, وتجسّدها في الداخل والخارج.
- السياسة الخارجية, عندما ينظر اليها على أنّها شرعية, ولها سلطة أخلاقية.

ومؤخرا, قدّم ناي مصطلح "القوّة الذكية", للإشارة الى التكامل بين القوّة الصلبة والقوّة الناعمة, حيث دعا الى سياسة خارجية, تجمع بين الوجود العسكري, والتحالفات, والشراكة مع أصحاب المصلحة الواحدة, معتبرا أنّ الطريقة المثلى لأية دولة, لتطوير قوّتها, هي عبر الجمع بين استراتيجيات القوّة الصلبة, والقوّة الناعمة.

ويقول ***ناي*** : إنّ هناك طريقة لممارسة القوّة, أكثر جاذبية من الطرق التقليدية, حيث يمكن للدولة ان تحقّق النتائج المرجّوة في عالم السياسة, عبر جعل الدول الأخرى تريد اللحاق بها, أو توافق على أوضاع, تعطي التأثير نفسه. "هذا الوجه الآخر للقوّة, الذي يحدث عندما تجعل دولة ما, دولاً أخرى تريد ما تريده هي, هوما يسمّى بالقوّة الناعمة ***co-optive power*** ,مقارنة مع القوّة الصلبة ,أو القوّة عبر فرض الأوامر على الآخرين, للقيام بما تريده". يتم ذلك, عبر مصادر للقوّة, كالثقافة والعقيدة والمؤسسات.

ويروّج لفكرته, عبر التشديد على أن القوّة الناعمة مهمّة, بقدر القوّة الصلبة . فاذا استطاعت دولة ما, أن تجعل من قوّتها, تبدو في عيون الآخرين شرعية, ستلقى معارضة أقل لرغباتها. واذا كانت ثقافتها وعقيدتها جذّابتين, سيلحق بها الآخرون بإرادتهم. واذا استطاعت إيجاد معايير عالمية تتوافق مع مجتمعها, فستشعر بحاجة أقل للتغيير. واذا جعلت دولا أخرى, ترغب في التنظيم بالشكل الذي ترتضيه الدول المهيمنة, فسوف تخفّف من أعباء استخدام القوّة بالإكراه, أو بالقوّة الصلبة. فـ***ناي*** يقول: "إذا كان بالإمكان الحصول على النتائج المرجوّة, عبر جذب الآخرين ليريدوا ما تريده, ستنفق أقل على "العصا والجزرة", مشيرا الى القوّة الصلبة.

ويشير ***ناي***, الى أن التحوّل في القوّة يكمن في أن " استخدام القوّة الصلبة أصبح مكلفا, بينما ازدادت جاذبية أنماط القوّة الأخرى, الأقل تكلفة". [111] فالقوّة الناعمة, هي "مجّانيّة" اذا صحّ التعبير, بمعنى أنّها لا تتطلّب مصادر مادّية, وعواقبها محدودة في حال الفشل. كما شدّد على أهمية الأسلوب. فالتصرّفات المتعجرفة, قد تعطي نتائج عكسية, وتسبّب نفورا بدلا من الجذب. ولكنه ينبّه الى أنّ القوّة الناعمة قد لا

---

110 In his book *Soft Power: the Means to Success in World Politics* (2004b)

111 Nye, Soft Power, p:166-167

تكون نواياها سليمة أحيانا, معطيا "الدعاية" كمثال, عن القوّة الناعمة, قائلا: " إنّ ليّ العقول, ليس بالضرورة أفضل من ليّ الأذرع."[١١٢] فقد يخطئ البعض في فهم هذا المصطلح (بالاشارة الى القوة الناعمة) , وأنّ نجاح القوّة الناعمة يعتمد على عنصري: المصداقية والشرعية.[١١٣]

ولكن للقوّة الناعمة موارد أخرى ,لا يمكن إنكار تأثيرها. فمع وجود أكثر من نصف مليون تلميذ أجنبي, يتلقون تعليمهم سنويا في الجامعات الاميركية, يمكن القول, أنّ اميركا تصدّر أفكارها وقيمها, من خلال هؤلاء, والذين سيشكّلون فيما, بعد النخبة النافذة في دولهم.[١١٤]

هذا الأمر يدفعنا الى القول, إنّ الدولة التي لا تملك من مصادر القوّة الصلبة العسكرية والإقتصادية ما يكفي, عليها أن تأخذ بعين الإعتبار القوّة الناعمة ومصادرها, كوسائل بديلة للحصول على أهداف سياسية, وإقتصادية, محلياً وعالمياً. ويقدّم ***جين لي Lee Geun*** , دراسة عن وضع كوريا الجنوبية , التي لا تستطيع أن تتنافس مع غيرها من الدول الصناعية , كالولايات المتحدة, أو اليابان, أو المانيا, أو حتى الصين في مجال القوّة الصلبة. فاستخدام كوريا للحرب, أو لعقوبات اقتصادية ,هو أخطر من استخدامها للمقوّمات الثقافية, أو غيرها من المصادر. وينتقد نظرية ***ناي*** للقوّة الناعمة على أنّها تتركّز فقط على هدف سياسي واحد, وهو جعل الدول تلحق بالقيادة الاميركية بإرادتها, من خلال استخدام هذه الاخيرة لمصادر القوّة الناعمة, كالثقافة, والتعلّم, والإيديولوجيا.

هذا ويعدّد ***جين لي*** , في نظريته عن القوّة الناعمة, استخدامات خمسة لهذه القوّة, تبعا للأهداف التي يراد من خلالها تحقيقها[١١٥]:

- القوّة الناعمة لتحسين الأمن الخارجي, عبر إضفاء صورة عن الدولة, تعكس جاذبيتها وطابعها المحبّ للسلام, مقدّما كمثال,الصعود السلمي للصين , التي تقدّم نفسها للمجتمع الدوليّ, كدولة مسؤولة, تاركة وراءها إرثها الشيوعي.

---

112 Nye, J. S. (2011). The Future of Power, New York. *Public Affairs*, 51. p:81

113 The velvet hegemon- How soft power can help defeat terrorism by Joseph Nye http://foreignpolicy.com/2009/11/02/the-velvet-hegemon/

114 وفقا لتصنيف صادر عن مركز تصنيف الجامعات في العالم, ومن بين قائمة ضمت ١٠٠٠ جامعة، كانت النسبة الأكبر منها من نصيب الولايات المتحدة الأميركية، حيث تصدرت ٢٢٤ جامعة بأميركا القائمة منها المراتب العشرة الاولى في التصنيف، بالإضافة إلى ٩٠ جامعة في الصين، و ٧٤ في اليابان، و٦٥ في المملكة المتحدة http://cwur.org/2016.php.

115 Geun, L. (2009). A soft power approach to the "Korean wave". *The review of Korean studies*, *12*(2), 123-128.

- القوّة الناعمة لحشد دعم الدول الأخرى, لسياسات الدولة الأمنية الداخلية والخارجية, على أن يكون لهذه السياسات, تبرير منطقي, من مثل الذي يعطي عقوبات إقتصادية, التي تعقب الغزوات الخارجية, وذلك عبر تدابير تتخذها الامم المتحدة, من خلال القرارات الصادرة إمّا عن الجمعية العامة ,أو عن مجلس الأمن. هذه الفئة من القوّة الناعمة ذات أهمية, لجهة توفير التكاليف حسب منطوق القوة الصلبة, لأن الشركاء في التحالف, يتقاسمون الأعباء.
- القوّة الناعمة لتغيير تفضيلات وطرق تفكير الدول الاخرى, من خلال نشر نظريات ومفاهيم تتبناها الدول, كالنيوليبرالية, والعولمة التي نشرتها القوى الانغلو- اميركية .
- القوّة الناعمة لتوحيد مجموعة من الدول, كلغة واحدة, أو تقاليد مشتركة, أو اسلوب عيش مشترك, كجهود الاتحاد الاوروبي, لتأسيس مجتمع اوروبي مشترك.
- القوّة الناعمة للحصول على التأييد والدعم المحليين للقائد, أو الحكومة المحلية.هذه القوّة تتّجه الى المجتمع الداخلي, من خلال خلق أبطال قوميين, والحث على القومية والوطنية, عبر المنافسات الرياضية العالمية ,أو إظهار الأداء المميز لقائد شعبي, في مؤتمر عالمي, لزيادة شعبيته.

لقد تعرّضت نظرية ***ناي*** حول القوّة الناعمة, لانتقادات كثيرة. فالبعض اعتبرها وسيلة من وسائل الهيمنة الامريكية, بينما سأل البعض الآخر أمثال ***جانس بياللي ماترن Janice Bially Mattern*** , " لماذا القوّة الناعمة ليست بناعمة كثيرا؟"[١١٦] وأضافت ***ماترن,*** إنّ القوّة الناعمة, هي امتداد للقوّة الصلبة, ولكن بوسائل مختلفة. كما أنها شكّكت بعبارة "الجاذبية", التي تحملها القوّة الناعمة, ورأت فيها عنصرا من الإكراه لا الجذب, وأنّ ***ناي*** لم يوضح من أين تأتي هذه الجاذبية. أما أستاذ التاريخ في جامعة هارفرد, ***نيال فيرغسون Niall Ferguson ,*** فأوضح أنّ الولايات المتحدة الأميركية, هي قوة عظمى, بسبب قدراتها العسكرية, التي هي جزء من القوّة الصلبة, كذلك الميزانية الهائلة المخصّصة للدفاع , كما أن القوّة الناعمة, هي أنعم من أن تحقّق المصالح الوطنية للولايات المتحدة. فبالرغم من أن معظم الشركات المتعدّدة الجنسيات, هي أمريكية المصدر,لكنها لم تستطع جعل الحضارة الامركية جذّابة كفاية ,معطيا أمثلة عن كون الاطفال في العالم الاسلامي, يستمتعون بالكوكاكولا والماكدونالدز, والافلام والموسيقى

116 Mattern, “Why ‘Soft Power’ Isn’t So Soft

الاميركية, لكن ذلك لم يجعلهم مغرمين بالولايات المتحدة الاميركية.[117] حتّى أن ***ناي*** نفسه, يعترف أنّ " موارد القوّة الناعمة مبعثرة, وبطيئة, ومعقّدة, مقارنة مع موارد القوة الصلبة".[118] ويضيف نقّاد آخرون بأنها غير ملموسة, ويصعب تحديد ما إذا كان لها تأثير يذكر. ففي حين أن نتائج الغارة الجويّة واضحة," لا يتضح ما اذا ما كان للقوّة الناعمة تأثير جوهري, في نتائج اتّباع سياسة معيّنة".[119]

ورغم هذه الإنتقادات التي وجّهت للقوّة الناعمة, وظهور هذه الأخيرة في سياق جغرافيّ, وتاريخيّ, وسياسيّ معيّن , الاّ أنّ المفهوم لاقى انتشارا واسعا بين صانعي القرار, ليصبح تعبيرا شائعا للإشارة الى الوسائل البديلة المتاحة للدولة, التي تسعى الى زيادة نفوذها وتأثيرها العالميين. وقدّم, ***ويندسور Smith windsor*** على سبيل المثال, خلاصته حول القوّة الناعمة, على أنها قد تمثّل إمّا وسائل بديلة للقوة العسكرية, وأمّا مكمّل لها.[120] كذلك ذكر ***روبرت كوبر Robert Cooper,*** حالات تاريخية متعدّدة,[121] تبدأ من" حصول "البابا", كمرجعية دينية, على طاعة شريحة كبرى من سكان العالم, حيث كان مرجعاً للشرعية, ومصدراً للقوّة الناعمة في عالم الإقطاعية", وتمر با***لناتو Nato***, والذي" يبدو وكأنه منظمّة ناعمة, ولكن هناك الكثير من القوّة الصلبة في أفعاله, "ليستنتج أنّ " القوّتين الصلبة والناعمة, هما وجهان لعملة واحدة,"[122]موضحا أنّه يمكن للدول, من خلال عدة وسائل, أن تحقّق أهدافها.

إنّ القوّة الصلبة والقوّة الناعمة في عالم اليوم تتفاعلان , وتتساندان, وأحيانا تتداخلان. ورغم أنّ القوّة الصلبة, عسكرية كانت أم اقتصادية, تحقّق, من خلال العنف, نتائج بوقت أقل, ولكن لفترة قصيرة الأمد, مقارنة مع القوّة الناعمة, فإن هذه الأخيرة, من خلال الإقناع والجذب, تحقّق تغييرات إرادية, على المدى

---

117 Ferguson, N.(Nov,2009)"Think Again: Power", Foreign Policy, available at: http://foreignpolicy.com/2009/11/03/think-again-power/

118 Nye Jr, J. S. (2004). The benefits of soft power. *Harvard Business School Working Knowledge*, *2*, 3. http://hbswk.hbs.edu/archive/4290.html

119 Hackbarth, J. R. (2008). *Soft power and smart power in Africa*. Naval Postgraduate School Monterey CA Center for Contemporary Conflict.p:4

120 http://www.journal.forces.gc.ca/vo1/no3/doc/50-56-eng.pdf

121 Cooper, R. (2004). Hard power, soft power and the goals of diplomacy. *American power in the 21st century*, 167-169

122 Ibid,p:175

الطويل. وقديماً قال ***ماكيفالي Machiavelli*** , "أن يخشاك الآخرون يجعلك في مأمن أكثر ممّا لو وقعوا في هواك". واليوم في عالم المعلوماتية, الأمران مطلوبان, الخوف والحب معا.[١٢٣]

ويقول ***غالاروتي Gallarotti***, "إنّ التشديد في الوقت الراهن على القوّة الناعمة, ما هو إلاّ رد فعل على المبالغة في إصدار القرارات المبنيّة على القوة الصلبة, وإهمال النتائج الايجابية, الناجمة عن استخدام القوة الناعمة ".[١٢٤] وطرح ***غالاروتي*** , في كتابه "القوّة الكونية في العلاقات الدولية", إمكانية قيام الدولة بتقوية نفوذها, عبر إقامة توازن بين القوّة الصلبة, والقوّة الناعمة, من خلال المزج بين نظريات العلاقات الدولية الثلاث, الواقعية المهووسة بالقوة, والليبرالية, والبنائية, اللتين تذهبان بعيدا في رفضها ", مع العلم, أنّ الأمر ليس هو نفسه بالنسبة لكلّ الليبراليين. فالليبرالي, ***جون ايكنبيري G. John Ikenberry*** مثلا, يصف النظام العالمي بعد الحرب العالمية الثانية, بأنّه "مزيج مميّز من الأمر والتبادل, ومن الإكراه والموافقة". هذا المزج مطلوب ,لأنّ تطبيق كلّ نظرية على حده, لم يعط النتيجة المرجوة, لجهة تقوية نفوذ الدولة.[١٢٥] وينطلق ***غالاروتي*** بنظريته هذه, من أنّ الإستعمال المفرط للقوّة الصلبة, يؤدي الى التقهقر الذاتي, والدول القويّة الفائقة الثقة بالنفس, تنخرط بتحدّيات خارجية كثيرة. ويرى أن القوّة الناعمة يساء فهمها, وأن المحاكاة هي تطبيق للقوّة الناعمة. هذه النظرية تتشابه مع نظرية القوّة الذكية التي أطلقها ***ناي*** , والتي استخدمتها ***هيلاري كلينتون Hillary Clinton*** وزيرة الخارجية الاميركية, ومرشّحة الحزب الديمقراطي لرئاسة الجمهورية, للإشارة الى حاجة الولايات المتحدة الاميركية, الى كل أساليب القوّة والنفوذ العسكري, والدبلوماسي, والثقافي, والانساني, والتكنولوجي, في سياستها الخارجية ,والحاجة الى تركيب مزيج خاص من القوّة الصلبة والقوّة الناعمة, يتماشى مع أوضاع معيّنة.[١٢٦]

---

123 Armitage, R. L., & Nye, J. S. (2007). *CSIS Commission on Smart Power: a smarter, more secure America*. P:6

124 Gallarotti, G. M. (2011). Soft power: what it is, why it’s important, and the conditions for its effective use. *Journal of Political Power*, *4*(1),p:43

125Gallarotti, G. M. (2010). *Cosmopolitan power in international relations: a synthesis of realism, neoliberalism, and constructivism*. Cambridge University Press.

126 http://www.cfr.org/counterterrorism/clintons-speech-smart-power-approach-counterterrorism-september-2011/p25854

فقرة ثالثة: القوّة الذكية

منذ صياغة ***ناي*** لمفهوم القوة الذكية,[١٢٧] والجدل مستمر حول الطريقة الأفضل, لإدماجها بالشؤون الوطنية والخارجية للدول. وأطلق ***ناي*** هذه العبارة عام ٢٠٠٣, كردّ على الفهم الخاطئ الذي لحق بمفهوم القوّة الناعمة, والتي قدّمها سابقا كبديل لاستخدام القوّة الصلبة, في السياسة الخارجية للرئيس الأميركي جورج بوش, والتي اعتبرها البعض انها قادرة وحدها على التأثير, في السياسة الخارجية للدولة.[١٢٨]

واعتبر ***ناي***, أنّ الاستراتيجيات الفاعلة في السياسة الخارجية اليوم, هي مزيج من القوّتين الصلبة و الناعمة, وهذا ما يطلق عليه القوة الذكية. فتوظيف القوّة الصلبة دون الناعمة, أو العكس, في ظرف معيّن, عادة ما يثبت عدم ملاءمته, معطيا "الإرهاب" كمثال, حيث تتطلّب مكافحته إعتماد استراتيجية القوة الذكية, إن لم يكن استخدام القوّة الناعمة ليدفع "طالبان" , الى أن تسلّم المواقع التي تستخدمها "القاعدة". فاللجوء الى القوّة الصلبة, كان أمراً حتميا. ولكن الأمر مغاير عندما يتعلق بالتعامل مع المسلمين المتشددين. القوّة الناعمة هنا ضرورية, لكسب قلوبهم وعقولهم, للحؤول دون تمكن المنظمات الإرهابية, من ضمّهم الى صفوفها.[١٢٩]

ويقول ***ناي,*** إنّ الاستخدام الناجح للقوة الذكية, سيقلل من حمى التسلّح أو الهيمنة, لا بل بالأحرى, ستجد طرقا لتجمع المصادر في استراتيجيات ناجحة, في سياق جديد لمفهوم انتشار القوة, و"نهوض الآخر".

إن نجاح استراتيجية القوّة الذكية, سيعطي إجابات على الأسئلة الآتية: ما هي الأهداف او النتائج التي يفضّل تحقيقها؟ ما هي المصادر المتوافرة ,وفي أي سياق ستستخدم؟ ما هو موقع وغايات الطرف

---

[127] The origin of the term "smart power" is under debate and has been attributed to both Suzanne Nossel and Joseph Nye, Deputy to Ambassador Holbrooke at the United Nations during the Clinton administration, is credited with coining the term in an article in Foreign Affairs entitled, "Smart Power: Reclaiming Liberal Internationalism", in 2004.

[128] Nye Jr, J. S. (2009). Get smart: Combining hard and soft power. *Foreign Affairs*, 160-163

[129] Gavel, D. (2008). Joseph Nye on Smart Power. *interview with Joseph S. Nye, Harvard Kennedy School Insight Interview*, *3*.
http://belfercenter.ksg.harvard.edu/publication/18419/joseph_nye_on_smart_power.html

المطلوب التأثير عليه؟ أي شكل من أشكال القوة لديه الفرصة بالنجاح أكثر من غيره؟ ما هي احتمالات النجاح؟

ويعرّف "المركز الأمريكي للدراسات الاستراتيجية والعالمية" القوة الذكية, بأنها "مقاربة تشدّد على أهمية وجود قوّة عسكرية, ولكن بالتزامن مع أهمية الاستثمار في إقامة التحالفات, والشراكات, والمؤسسات على الأصعدة الكافة, لتوسيع النفوذ الأميركي, وإعطاء الشرعية للأفعال الأميركية ".[١٣٠]

أما ***شستر كروكر Chester Crocker ,*** فيعرّف القوّة الذكيّة, بأنها "استراتيجية استخدام الدبلوماسية, والإقناع, وبناء القدرات, وفرض السلطة والنفوذ, بطرق مؤثرة, ولها شرعية سياسية واجتماعية, عبر إشراك القوّة العسكرية, وكل أشكال الدبلوماسية".

أمّا ***ويلسون,*** فيعرّفها, بأنّها "قدرة اللاعب على جمع القوتين الصلبة والناعمة معا, بحيث أنّ كلّ قوّة تدعم الأخرى, صوب تحقيق غايات اللاعب, بكفاءة وفعالية ". كما أنّه وجد أن القوّة الذكيّة, تستخدم بفعالية أكثر, الأدوات العسكرية والاقتصادية والناعمة, لحل المشاكل وادارة الحوار, عندما يتم فهم الهدف المعني, والسياق الاقليمي والعالمي. لكنّ ***ويلسون*** يستخلص, أن ما يعتبر "ذكياً" في سياق معيّن, يمكن أن لا يعطي النتيجة نفسها, في سياق آخر. فاستراتيجية ذكيّة في افغانستان, قد لا تكون استراتيجية ذكيّة في العراق, فكل أداة قوّة, لديها توقيتها. فالقوّة الناعمة, قد تستغرق سنوات لتحقق نتائج معيّنة, في حين أنّ القوّة الصلبة, كغارة جوّيّة, تعطي نتائج أسرع. فعاملا الوقت والجغرافيا يحدّدان, ما اذا كانت الاستراتيجية المتبعة, ذكيّة أم لا.[١٣١]

ويضع ***ويلسون*** شروطاً, لا بد من توافرها, لتحقيق القوة الذكية:

- تحديد الهدف من ممارسة القوّة. فالقّوة لا يمكن أن تكون ذكيّة دون أن يعرف ممارسوها الهدف من استخدامها, كذلك الشعوب والمناطق المستهدفة منها.
- الإدراك والفهم الذاتي للأهداف, بالموازاة مع القدرات والإمكانيات المتاحة. فلا يمكن للقّوة الذكيّة أن تعتمد على الأهداف, دون تحديد عنصري الإرادة والقدرة على تحقيقها.
- السياقان الإقليمي والدولي, الذي سيتم في نطاقهما تحقيق الأهداف.
- الأدوات التي سيتم استخدامها, بالإضافة إلى توقيت وكيفية توظيفها منفصلة أو مع غيرها.

[130] Armitage, R. L., & Nye, J. S. (2007). *CSIS Commission on Smart Power: a smarter, more secure America*. CSIS, P:7

[131] Wilson, ,"Hard power, soft power, smart power",p:115-123

فالقوّة الذكيّة, ليست فقط امتلاك المصادر الناعمة والصلبة, والمزج بينهما, بل القدرة على تحديد وقت استخدامها. وأيّ منهما يفضّل استخدامه في الموقف, والقدرة على تحديد متى يتم الدمج بينهما, وكيف يتم الدمج. فالاتجاه المركب لتفسير القوّة, من خلال القوة الذكية, يعنى التعامل مع عناصر القوة الناعمة والصلبة, ليس على أساس كونهما منفصلين, بل على التعامل معهما ككل, والتعامل مع التداخل القائم بينهما.

فليس هناك وصفة سحرية لتطبيق القوة الذكية, ولم يحدّد ناي استراتيجية محددة لخلق القوة الذكية, وإنما وفقا للشروط السابقة, يستطيع كل لاعب أن يحدّد استراتيجيته, ويرسم خطوطها الأساسية, طبقا لثلاثية الأهداف, والوسائل, والسياق الذي يحدّد ما أسماه ***ناي*** الاستراتيجية الكبرى, التي تجمع بين أدوات القوة الناعمة, والصلبة, وتمثّل القيادة السياسية والموقف الشعبي.[١٣٢]

وعرض ***ويلسون*** لمجموعة من التحديات, التي تقف في وجه استخدام القوّة الذكية, والقدرة على إنجاحها. وتنقسم هذه التحديات إلى:

أولاً :التحدّي المؤسّسي:

يتمركز التحدّي المؤسّسي للقوة الذكية في الفجوة القائمة بين مؤسسات القوة الصلبة المتمثلة في المؤسسة العسكرية, التي تعتمد على استخدام الإكراه, وبين مؤسسات القوّة الناعمة, التي تفتقد الى الاهتمام والدعم الكافيين, من قبل الدولة. فحجم مؤسسات القوة الصلبة, أكبر بكثير من تلك المخصصة للقوّة الناعمة, ما يؤثّر في أدائها, وبالتالي في أداء القوّة الذكيّة. فهذا يعني, بشكل أو بآخر, أنّ مؤسّسات القوّة الناعمة, تكون خاضعة, إلى حدّ ما, لمؤسّسات القوّة الصلبة, كالمؤسّسة العسكرية والمخابرات, التي قد تحدّد ما يفعل, أو ما لا يفعل, على صعيد القوة الناعمة. كما أن الثقافة المؤسسية للمؤسسات الأمنية, بشكل عام, قد تمثّل معوقا لأي تعاون, قد يحدث بين مؤسسات طرفي القوّة, وهو ما يؤثر سلبيا وبشدة على تحقيق القوّة الذكيّة, بشكلٍ مثمر.

ثانياً: التحدّي السياسي:

إنّ القوة الذكية لا تحتاج فقط الى مؤسسات تدعمها وحسب, بل تحتاج إلى قوّة سياسية, وإرادة من القيادة لتحقيقها. فالجانب المؤسّسي يعتمد في إصلاحه, بالأساس, على مثل هذه القيادة الراغبة. كما أنّ غياب التوازن السياسي بين القوة الناعمة, والقوة الصلبة, يشكّل تحديّا آخراً, من تحديات القوة الذكية. فأنصار

[132] Ibid,p 115-118

القوة الصلبة ومؤيّدوها, أكثر قوة, وحجمًا, وتمثيلًا, من أنصار القوة الناعمة, وهذا لا يقتصر على النخبة السياسية للدولة, بل يمتد الى دوائر الجماهير, والتأييد الشعبي لها. فالناخبون السياسيون, عندما يختارون ممثّلا لهم, إنّما يفضّلون التوجّه الذي يعتمد على القوة الصلبة, المرئية والملموسة, التي يأخذها هؤلاء في الاعتبار, ويعتبرونها رمزا لقوة الدولة, وتأثيرها, ومقدرة على حماية مصالحها. فأنصار القوّة الناعمة بين فئات المواطنين, أقل بكثير, من هؤلاء المؤيّدين للقوّة الصلبة, بحيث يقتصر التأييد والدعوة لهذا التوجه, على فئات الأكاديمين والدبلوماسيين السابقيين, فلا يوجد قوة شعبية, توازن تلك التي تمتلكها القوة الصلبة.[١٣٣]

إن مفهوم القوة الذكية لم يخل من الانتقاد, من حيث تعريف كل من القوتين الصلبة والناعمة, كلّ على حده, فـ***ماترن*** ترى, أنّ "اللغة" التي تعتبر من أدوات القوّة الناعمة, يمكن أن تستخدم بطريقة تحمل معاني الإكراه, والعنف , مقدمة "الحرب على الإرهاب", كمثال على ذلك. فعندما توجّه الرئيس الاميركي ***جورج بوش*** بهذه العبارة الى العالم, أوحى بذلك أن الدول إما أن تكون مؤيّدة, وإما تعتبر"إرهابية". فهذه العبارة ,على حد قول ***ماترن***, وضعت فخّا يحتوي على "لا خيار آخر". إنّ الرسالة التي أوصلتها هذه العبارة الى الدول, هي أنّها اذا أرادت ان تعتبر الى جانب الخير, عليها أن تساند الحملة الاميركية على الإرهاب. ولكن من الواضح, أنّها كانت توحي, أنّ الخيار الآخر يساوي دعم "الإرهابيين", وهذا ما جعل دولا مثل الأردن مصر, وتركيا, تفضّل الجانب الأميركي في تعاملها الدولي, لأنها كانت تريد أن تؤسّس لموقعها كدول " خيّرة", لا العكس.[١٣٤]

من ناحية أخرى, إنّ القوّة العسكرية, يمكن أن تكون أكثر جاذبية أحياناً, لا سيّما في حالات التدخّل الانساني او حفظ السلام, بحيث تستخدم على شكل قوّة ناعمة, لأن الشعوب تميل الى تقبّل هذا النوع من المساعدة, حتى لو حملت في طيّاتها استخداما للعنف. والأمر نفسه يمكن أن يقال, بالنسبة لأدوات القوّة الناعمة. فقد يتجاوز التبادل الثقافي, أو الاكاديمي, أو حوار الحضارات, حدوده في السعي الى تشجيع التواصل والتقارب بين الشعوب, الى أهداف الترويج لعقيدة, أو حضارة معينة, سعيا لترسيخها, في أذهان الشعوب[١٣٥].

---

133 Ibid, p,118-120

134 Mattern, WhySoft Power'Isn't So Soft,p:590

135 Cross,Europe as a Smart Power,p:11

وترى **دافيس كروس Davis cross** أنّه لا معنى في تعريف القوّة الذكيّة, بأنّها "الجمع الفعّال بين القوتين الصلبة والناعمة", الاّ اذا حذفت كلمة "الفعالية" من التعريف, ليعاد تعريف القوّة الذكيّة, بأنها "استراتيجية استخدام الإكراه والاستمالة بشكل متزامن", ما يمكّن الأكاديميين, من التفرقة بين محاولات استخدام القوة الذكية وبين نتائجها النهائية ,التي قد تكون فاعلة أو غير فاعلة, أو ما بين بين. [١٣٦]
وتعتبر الدبلوماسية العامة, ووكالات الاستخبار, ونشر ثقافة وفنون الدولة في الخارج, و شبكات الإنترنت, والإعلام, من أدوات القوّة الذكيّة.

المطلب الثالث: تصنيف القوّة السيبرانيّة:

لقد ركّزت الاستراتيجيات الأمنية في الفضاءات المتعدّدة, على تطبيق إحدى القوّتين, إما الصلبة منها, كالإكراه مثلا, أو من خلال استخدام أساليب القوّة الناعمة. أمّا في الفضاء السيبراني, فالأمر يطرح إشكالية لجهة تصنيف القوّة السيبرانية, ضمن مجالي القوّة الناعمة أو القوّة الصلبة. فغالبا ما كان العالم الرقمي يقارن بالقوّة الناعمة, لكن تصاعد العنف في الفضاء السيبراني, دفع نحو إدراك مختلف للقوة السيبرانية. فعلى صعيد القوة الناعمة, تمتلك محركات البحث على شبكة الانترنت, مثلا, تأثيرا اكبيرا على الأفكار. تجعلها أداة من أدوات هذه القوة, حيث تشكّل هذه المحرّكات, أداة جذب قوية للمستخدمين. فمحرّك البحث **غوغل google** ,مثلا, يستحوذ على ٨٣% من السوق العالمي,(يليها محرك البحث **ياهو yahoo** ثم **بيند Bind** و **بايدو الصينيBaidu**),[١٣٧]حيث يقدّم أكثر من تريليون عنوان على شبكة الانترنت, كنتيجة لعمليات البحث التي يقوم بها المستخدم, على هذا المحرك. وبما أنّ المستخدم عادة ما يختار, أول ثلاث أو خمس نتائج للبحث, فقد أصبح غوغل, بالتالي, قادرا على تشكيل التفضيلات, عبر تقريره لما هو مهم, وما هو غير ذلك.
كذلك إنّ استخدام الفضاء السيبراني في إدارة العمليات النفسية, والتأثير في الرأي العام, وتكوين التحالفات الدولية, وفي عمل أجهزة الاستخبارات الدولية, بما وفره من سيل عالمي من المعلومات, لا يقتصر على وجهة النظر الرسمية للدول والحكومات فقط, بل تعداه ليعطي الأفراد دورا في إنتاج المعلومات, وفي

---

136 Ibid,p:12

137 "Desktop Search Engine Market Share", April2013
http://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0
(last visited august 20,2016)

توافر كمّ هائل من التحليلات السياسية والاقتصادية, متعديا الحدود الدولية, ومشكلا ثورة معلوماتية هائلة, لا حدود لها, لطالما عكفت أجهزة الاستخبارات الكبرى على الرجوع اليها للبحث فيها, وتوظيف نتائجها.[١٣٨]

ويعتبر***شلدون,*** أنّه يمكن استخدام أدوات المعلومات داخل الفضاء السيبراني, لإنتاج قوّة ناعمة, من خلال وضع خطة, ومن خلال الجذب والإقناع. مثل جذب البرمجيات الحرّة, والمفتوحة المصدر. ولكن, بإمكان الموارد السيبرانية, أن تنتج قوّة صلبة في الفضاء السيبراني. فاللاعبون, من دول ومن غير دول, يمكنهم إطلاق هجمات منظّمة لتعطيل الخدمة, باستخدام ما يسمّى بِ***botnet (***zombiemalware) من مئات الالآف من الكمبيوترات الخبيثة, التي تجتاح شركة, أو نظام الإنترنت, في دولة ما, وتعطّل عملها. وحيث إنّ عملية إدخال الفيروس, في الكمبيوترات الغير المحصّنة, هي عملية غير مكلفة. ويتم إنتاج القوّة الصلبة,أحيانا, في الفضاء السيبراني, من خلال القراصنة النشطاء ***hactivist***, كما هو حال القراصنة الصينيين, اللذين يقومون بأعمال تخريبية, في المواقع الالكترونية التابعة للتايونيين. وبالمقابل, يقوم القراصنة التيوانيون, بتخريب المواقع الإلكترونية الصينية. كما يعتبر إدخال شيفرة خبيثة لتعطيل الأنظمة, أو لسرقة ملكية فكرية, مثالا على القوة الصلبة السيبرانية.

أما خارج الفضاء السيبراني , فانسياب المعلومات السيبرانية, من شأنه أن يخلق قوة ناعمة, عبر جذب مواطني دولة أخرى, كالقيام بحملة دبلوماسية عامة عبر الإنترنت . لكن يمكن للمعلومات السيبرانية أن تصبح مصدرا لقوة صلبة, من شأنها إلحاق الضرر بأهداف مادية لدولة أخرى, خاصة وأنّ الكثير من الصناعات, والمرافق الحديثة, لديها عمليات متصلّة بأنظمة ***SCADA*** .[١٣٩]

وبنظر ***ناي***, فإن الأدوات المادية, يمكن أن تؤمّن موارد قوّة, لها علاقة بالفضاء السيبراني, فالموجّهات, والخوادم, وكابلات الألياف البصرية التي تحمل إلكترونات الإنترنت, لها موقع جغرافي تحت ولاية الحكومة. والشركات التي تستخدم الإنترنت, تخضع لقوانين هذه الحكومات. ويمكن لهذه الأخيرة, أن تمارس قوة إكراه تجاه الشركات والأفراد. فالملاحقة القانونية, حملت ياهو***yahoo***, على ضبط ما يرسله الى فرنسا, وجعلت ***غوغل Google ,*** يحذف خطابات الكراهية من عمليات البحث في المانيا. كما أنّ الحكومات تسيطر على الإنترنت, من خلال تهديد الوسطاء, كمقدّمي خدمات الإنترنت, والمتصفّحات,

---

[138] عادل عبد الصادق,الإرهاب الإلكتروني القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة,المركز العربي لأبحاث الفضاء الالكتروني,الطبعة الثانية,القاهرة, ٢٠١٣ ,ص٤٧

[139] Nye, *Cyber power,p:7*

ومحرّكات البحث, والوسطاء الماليين. ويرى ***ناي*** أن الأدوات المادية, يمكنها أن تؤمّن موارد من القوّتين الناعمة والصلبة في آن معا. فالمعلومات السيبرانية, ترتكز الى بنية تحتية,هي عرضة لهجوم عسكري مباشر, أو تخريب من قبل الحكومات, ومن قبل اللاعبين من غير الدول, كالإرهابيين والمجرمين, بحيث يمكن تفجير الخوادم, أو قطع الكابلات. وفي مجال القوّة الناعمة, إنّ اللاعبين من غير الدول, والمنظّمات الغير حكومية, يمكنها تنظيم إحتجاجات ضد الشركات, والحكومات, التي تعتبر أنها تسيء إستخدام الإنترنت. ففي عام ٢٠٠٦, نظّم متظاهرون مسيرة في واشنطن, ضد ***ياهو***, وغيرها من شركات الإنترنت, التي كانت تمدّ الحكومة الصينية بأسماء الناشطين الصينين,الأمر الذي تسبّب في اعتقالهم. كما يمكن للموارد المادية, أن تخلق قوة ناعمة, من خلال إعداد بعض الحكومات لخوادم وبرمجيات, من شأنها مساعدة الناشطين في مجال حقوق الإنسان, على نشر رسالتهم, رغم محاولات حكوماتهم قمع ذلك, عبر إنشاء جدران الحماية, لمنع هذه الرسائل من الإنتشار. وهذا ما فعلته الحكومة الايرانية, لقمع المحتجين عقب انتخابات عام ٢٠٠٩, بعد أن قامت الحكومة الأميركية بتطوير البرامج والأجهزة, التي تمكّن هؤلاء من نشر رسائلهم.

كما ينظر ***ناي***, الى القوة السيبرانية, كقوّة صلبة وناعمة في الوقت نفسه, من حيث الأوجه الثلاثة للقوّة:

فقرة أولى: التخلّي عن التفضيلات الأساسية

هو إمكانية اللاعب على حمل الآخرين, على القيام بما هو مغاير لتفضيلاتهم الأساسية, أو لإستراتجيتهم.[١٤٠] حيث تتمثّل القوّة الصلبة هنا, بحجب الخدمات التي ذكرت أعلاه. واعتقال أو منع المدوّنين المنشقّين, من نشر رسائلهم. ففي عام ٢٠٠٩, حكمت الحكومة الصينية, على ناشط ومدوّن صيني, بالسجن إحدى عشرة عاما ,لقيامه بالتحريض على تقويض قوة الدولة. كما أدخلت قيودا جديدة على التسجيل في المواقع الإلكترونية, وعلى العمليات التي يستخدمها الأفراد.[١٤١] أما القوّة الناعمة, فتتمثّل في محاولة الفرد أو المنظمة, إقناع الآخرين بتغيير سلوكهم. فالحكومة الصينية, إستخدمت أحيانا الإنترنت, من أجل حشد الطلاب الصينين, للتظاهر ضد اليابان, بعد المواقف التي علنها المسؤولون اليابانيون والتي إعتبرتها الصين مهينة لها. كما أن الأفلام التي ينتجها تنظيم القاعدة على الإنترنت,

[140] Ibid, p:8

[141] "Don't mess with us," The Economist, January 2, 2010, 31

والمعدّة من أجل تجنيد الناس لخدمة قضيته, هي حالة أخرى من القوّة الناعمة, المستخدمة لتحويل سلوك الأفراد عن تفضيلاتهم أو استراتيجتهم الاصلية.

فقرة ثانية: وضع الأجندة

هو وضع الأجندة, حيث يمنع اللاعب خيارات لاعب آخر. فإن حصل ذلك عكس إرادته, أعتبركنمط من أنماط القوة الصلبة , أما إذا حصل الأمر برضاه فإنه يعتبر والحالة تلك نمطا من أنماط القوة الناعمة. فعام ٢٠١٠ مثلا, وفي ذكرى الثورة الإيرانية , قامت الحكومة الإيرانية بإبطاء سرعة الإنترنت, وذلك لمنع المحتجّين من إرسال أفلام إحتجاجهم عبر اليوتيوب ***youtube***. فبحسب "مبادرة الشبكة المفتوحة", هناك على الأقل, أربعون دولة تستخدم الفلترات, وجدران الحماية, لمنع المناقشات في مواضع تثير الريبة. فبعض هذه الدول, يفرض رقابة سياسية, وأخر يحجب مضامين لأسباب إجتماعية, كتلك المتعلّقة بالجنس والميسر والمخدرات. حتى أنّ الولايات المتحدة, وبعض الدول الأوروبية تقوم بذلك إنتقائيا.[١٤٢] وفي بعض الأحيان, ما يبدو قوة صلبة للبعض , قد يبدو قوة ناعمة للآخرين. فعندما قاضت صناعة الموسيقى, أكثر من ١٢٠٠٠ أمريكي, لسرقتهم الملكية الفكرية, بتحميلهم للموسيقى من شبكة الانترنت, بطريقة غير شرعية, إعتبر الذين تمت مقاضاتهم الأمر بمثابة قوّة صلبة, لكن عندما عمدت شركة مثل ***أبل Apple***, الى عدم السماح لبعض التطبيقات بالتحميل عبر هواتفها, لم ينتبه الكثيرون لذلك.

فقرة ثالثة: الإنخراط في تشكيل تفضيلات لاعب آخر

يتعلّق بلاعب ينخرط في تشكيل تفضيلات لاعب آخر, الى حد أن بعض الإستراتيجيات ,لا تؤخذ بعين الاعتبار. فعندما اختارت شركات أن تضع كودا بدلا عن آخر في انتاجها للبرمجيات , فإن القليلين من المستهلكين لاحظوا الامر. وقد تنظم الحكومات, حملات لنزع الشرعية عن أفكار معينة, كديانة ***الفالون غونغ Falun Gong*** في الصين, وتحظر نشر تعاليمها على الانترنت , بحيث يصعب على المواطنين الصينيين معرفة ذلك.أو عندما حجبت الحكومة السعودية عن مواطنيها, مواقع تعتبرها غير مؤمنة. وهذا

---

142 Waters, R., & Menn, J. (2010). Closing the Frontier. *Financial Times*. http://www.ft.com/cms/s/0/dc381fdc-3ac9-11df-b6d5-00144feabdc0.html?ft_site=falcon&desktop=true#axzz4ZGEhDmqe

دفع ايضا الولايات المتحدة الأميركية, الى اتخاذ إجراءات تتعلّق بشركات بطاقات الإعتماد المصرفية, بحيث جعلت لعب الميسر عبر الإنترنت, غير متوفّر لمواطنيها. أمّا فرنسا والمانيا, فقد منعتا مناقشة الأفكار النازية على الانترنت.[١٤٣]

وعليه يمكن اعتبار القوة في الفضاء السيبراني, نمطا من أنماط القوة الذكية, القائمة على المزج بين القوتين الناعمة والصلبة. ذلك أنّ الاعتماد على القوة الصلبة (العسكرية) منفردة, لا يؤدي الى إحراز الأهداف المتعلقة بالشأن السياسي الخارجي للدولة, وإنما يتطلّب المزيد من وسائل القوّة الناعمة القائمة على الإقناع والجذب, لإحداث التغيير في سلوك ومسارات تفكير الشعوب.

143 Nye *Cyber power*. p.6

المبحث الثاني: التكنولوجيا وأثرها في تحولات القوة

في الوقت الذي تشير فيه الأرقام والإحصاءات الى مدى توسّع استخدام تكنولوجيا المعلومات والاتصالات, الاّ أنّ المفكرين منقسمون حول مدى الدور الذي تلعبه, بحيث يركّز البعض على النواحي الايجابية, فيما يشدّد البعض الآخر على الآثار السلبية, ويبقى أنّها أنتجت قوّةً سيبرانيّةً, بمزايا متعدّدة لم تكن متوافرة من قبل.

المطلب الأول: تكنولوجيا المعلومات: ثورة صناعية ثالثة

أحدث تطوّر تكنولوجيا المعلومات, تحوّلا كبير في مفهوم القوّة, جعل المجتمع الدولي أمام مرحلة جديدة. فقد بات التفوّق في مجال الفضاء السيبراني, عنصرا حيويا في تنفيذ عمليات فاعلة, على الأرض, أو البحر, أو الجوّ, أوالفضاء, واعتماد القدرة القتالية في الفضاء السيبراني على نظم التحكّم والسيطرة. وقد أوجدت الأعداد الهائلة من أجهزة الكمبيوتر المنتشرة, عالما افتراضيا, نشأ نتيجة عملية الاتصال، ومثّل وسيطا جديدا للقوة, حيث يمكن للقراصنة دخول الفضاء السيبراني بهدف محاوله السيطرة على الأجهزة, وسرقة المعلومات, وإفسادها أو تعطيلها.[١٤٤]

ودخل العالم اليوم,العصر الرقمي, حيث الملفات الورقية, والمنتجات, والعمليات, أصبحت رقمية ومتوافرة من خلال شبكة الانترنت. هذه العملية, بدأت بالملفات النصية, وتوسعت لتشمل الصور, والمحاضرات , والأفلام, والخرائط وغيرها . حتى شكّلت نقلة نوعية في عالم الاتصالات .هذه المقاربة خفضت من التكلفة, وأمنت فرصا لتداخل المعلومات لم تكن ممكنة سابقا.

لقد حوّلت الإنترنت, رؤية ***مارشال ماكلوهان***, حول "قرية عالمية" والتي أطلقها في السبعينات, الى واقع.[١٤٥] فمنذ ١٩٩٤, توسّعت شبكة الإنترنت لتخدم ملايين المستخدمين, وغيّرت في سنوات قليلة,

---

[144] عبد الصادق, عادل ،أمريكا وتشكيل قيادة عسكرية في الفضاء الإلكتروني. هل بدأ الاستعداد لحروب المستقبل ؟ .تعلقيات مصرية ، مركز الاهرام للدرسات السياسية والاستراتيجية ، العدد١٣٠:١٢يوليو ٢٠٠٩

[145] Marshall McLuhan (1911–1980 is Canadian professor, philosopher, and public intellectual. His work is viewed as one of the cornerstones of the study of media theory, universally regarded as the father of communications and media studies and prophet of the information age)

طريقة التواصل في الميادين كافة, وأصبحت المصدر العالمي الأول للمعلومات. حتى أن الرئيس الاميركي السابق, ***بيل كلينتون Bill Clinton***, أشار الى سرعة نمو وانتشار الانترنت, بقوله:"عندما استلمت الحكم, فقط العلماء الفيزيائيون كانوا قد سمعوا بما يسمّى بالشبكة العنكبوتية العالمية... اليوم, حتى قطتي لديها صفحة".[١٤٦] واليوم, بلغ عدد مستخدمي شبكة الإنترنت في العالم (حزيران ٢٠١٦) ٣,٥٦٦,٣٢١,٠١٥ مستخدما, من أصل عدد سكان العالم البالغ ٧,٣٤٠,٠٩٣,٩٨٠, أي بمعدّل ٤٨.٦% .[١٤٧] كذلك يستخدم حوالي المليارين, وسائل التواصل الاجتماعي, الأكثر شعبية, مثل فيسبوك, الذي تخطّى عدد مستخدميه المليار,[١٤٨]وهذا الرقم الى تزايد, مع زيادة استخدام الهواتف الذكية.

كما جاء على لسان أحد المسؤولين الرسميين الاميركيين ", اليوم, يمكن القول, إنّ تكاثر المعلومات كما تكاثر التسلّح, هو سبب في انعدام الاحادية [١٤٩] .

لطالما تسبّب دفق المعلومات والتحكّم بها قلقاً للدول. ففي القرن الخامس عشر, شكّل اختراع ***غوتنبرغ Gutenberg*** لآلة الطباعة, وانتشار النسخ المطبوعة من الإنجيل المقدس, في قسم كبير من اوروبا, دورا اساسيا في انطلاق الاصلاح. ويطلق ***ناي***, على ثورة المعلومات, اليوم, " الثورة الصناعية الثالثة", كنتاج لسرعة التطور التكنولوجي في عالم الحواسيب والاتصالات, التي بدورها أدت الى النقص في كلفة خلق المعلومة, وانتاجها, ونقلها.

وعندما بدأ المسح السماوي الرقمي(SDSS),[١٥٠] العمل عام ٢٠٠٠, جمع تلسكوبه في مدينة نيومكسيكو, في الأسبوع الأول,من البيانات, أكثر مما تمّ جمعه في تاريخ علم الفلك. وبعد أكثر من عقد

---

146 CLINTON, B., & GORE, A. (1996). Excerpts from Transcribed Remarks by the President and the Vice President to the People of Knoxville on Internet for Schools. *Speech. Knoxville: White House*. http://govinfo.library.unt.edu/npr/library/speeches/101096.html

147 http://www.internetworldstats.com/pr/edi083.htm

148 http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

149 Haass, R. N. (2008). The age of nonpolarity: what will follow US dominance. *Foreign Affairs*, 44-56.R. N. Haass, (2008). https://www.foreignaffairs.com/articles/united-states/2008-05-03/age-nonpolarity

150 Sloan Digital Sky Survey or SDSS is a major multi-filter imaging and spectroscopic redshift survey using a dedicated 2.5-m wide-angle optical telescope at Apache Point

من الزمن, تم جمع أكثر من ١٤٠ ترابيت من المعلومات, في أرشيفه. هذا الكمّ من المعلومات, هو على الأرض ايضا. فعلى سبيل المثال, سعة المعلومات التي يتداولها ***وال مارت Walmart*** عملاق الجملة, مع أكثر من مليون زبون كل ساعة, تفوق ٢.٥ بيتابيت, أي ما يعادل ١٦٧ مرة, الكتب الموجودة في مكتبة الكونغرس الأميركي. كما أنّ حلّ رموز شفرة جينات الكائن الحي يتم إنجازها اليوم, في مهلة اسبوع.[١٥١]

أمّا ***فيسبوك Facebook***, فهو اليوم مقر لأكثر من ٤٠ بيليون صورة. ووفقا لبحث قامت بها شركة ***BMI***[١٥٢], فإنّ٩٠% من البيانات في العالم, تم جمعها في السنوات القليلة الماضية. فعلى سبيل المثال, يتم إرسال ٣٥٠,٠٠٠ تغريدة عبر تويتر, في الدقيقة الواحدة, كما يتم التعامل بملايين الدولارات, عبر موقع Amazon .[١٥٣]

فالثورة المعلوماتية الجارية, والتي تسمّى أحيانا "الثورة الصناعية الثالثة",[١٥٤] مبنية على التطوّر السريع للكمبيوترات والإتصالات, ونظم البرامج ,التي أدّت الى تناقص في تكلفة خلق, وإنتاج, ونقل المعلومات. ففي عام ١٩٩٣, كان هناك خمسون صفحة على الشبكة العنكبوتية, أما اليوم, فالرقم تخطّى المليار.[١٥٥] وعام ١٩٨٠, كانت الاتصالات الهاتفية عبر الأسلاك النحاسية, تحمل صفحة واحدة من المعلومات في الثانية, بينما اليوم, بإمكان سلك رفيع من الألياف الضوئية, يمكنه نقل ٩٠٠٠٠ مجلد, في الثانية. وعام

Observatory in New Mexico, United States. The project was named after the Alfred P. Sloan Foundation, which contributed significant funding.

151 Cukier, K. (2010). *Data, data everywhere: A special report on managing information*. Economist Newspaper.http://www.economist.com/node/15557443

152 International Business Machines Corporation (commonly referred to as IBM) is an American multinational technology and consulting corporation, with corporate headquarters in Armonk, New York. IBM manufactures and markets computer hardware, middleware and software and offers infrastructure, hosting and consulting services in areas ranging from mainframe computers to nanotechnology.

153 https://blog.dashburst.com/infographic/why-big-data-is-everywhere/December 5, 2013

154 Rifkin, J. (2011). *The third industrial revolution: how lateral power is transforming energy, the economy, and the world*. Macmillan.

155 http://www.internetlivestats.com/total-number-of-websites

١٩٨٠ , كان جيغابيت من التخزين بحاجة الى حجم غرفة, أمّا الان, فمئتا جيغابيت تسعا جيب القميص. فكمية المعلومات الرقمية, تزداد عشرة أضعاف, كلّ خمس سنوات.[١٥٦]

لقد أوجد التغيّر الكميّ تغيرا نوعيا . فمثلا, محرك البحث ***بينغ Bing***, يمكن أن يساعد الزبائن في شراء تذكرة سفر الآن, أو تأجيلها الى حين انخفاض الثمن, عبر تفحّص ٢٢٥ بليون سجل للأسعار, والرحلات, كذلك لغرف الفنادق, أو السيارات, أو غيرها.[١٥٧]

ويقول ***جيمس كورتادا James Cortada*** من ***IBM***, وهوالذي ألّف عددا من الكتب عن تاريخ المعلوماتية, " إننا في حقبة مختلفة, بسبب الكم الهائل من المعلومات". كما أسماها عالم الكمبيوتر **جو *هلرستاين***, من جامعة كاليفورنيا " بالثورة الصناعية للبيانات".[١٥٨]

ومما لا شك فيه, إنّ التطوّرات التقنية, أصبحت الإنطلاقة نحو التغيير. فإنخفاض التكلفة, وقوة آداء أجهزة الكمبيوتر, قد أدّيا الى استخدام تكنولوجيا المعلومات, في الميادين الحياتية كافة.

وتعرّف ***ميريام كافلتي Myriam Cavelty***, الثورة التكنولوجية "كظاهرة, تتكشّف عواقبها, في فضاء تشكلّه الآف المؤثّرات, والمؤسسات, والتقاليد, والثقافات, وغيرها, ذلك بالرغم من أن التطورات التي طرأت على تكنولوجيا المعلومات, هي التي أوجدت هذا الفضاء, وأدت الى استخدامه في كل النواحي الحياتية للمجتمع".[١٥٩]

كما يرى الليبراليون, أمثال ***جون بارلو***, أن" الثورة التكنولوجية هي قفزة تقنية الى الأمام, خلقت تحوّلا حتميا ودون عودة, في كافة نواحي الحياة".[١٦٠] ولكن بعض المراقبين, يشكّكون في مدى تأثير تكنولوجيا

---

156 NYE, J.(2013)The information revolution gets political -THE AUSTRALIAN http://www.theaustralian.com.au/news/world/the-information-revolution-gets-political/story-e6frg6ux-1226574887092

157 Cukier, K. (2010). *Data, data everywhere: A special report on managing information*. Economist Newspaper. http://www.economist.com/node/15557443

158 Toffler, A., & Toffler, H. (1995). *Creating a new civilization: The politics of the third wave*. Turner Pub.

159 Cavelty, M. D., & Mauer, V. (2016). *Power and security in the information age: Investigating the role of the state in cyberspace*. Routledge.p:4

160 Civil Society Information Society Advisory Committee. (2011). CSISAC statement on OECD communique on Internet policy-making principles. P: 5, www.oecd.org/internet/innovation/48289796.pdf

المعلومات, ويشيرون الى محدوديتها في تحسين الإنتاجية, وخلق تحوّل في الإقتصادات الصناعية, كذلك يحذرون من تبني النهج الحتميّ, لطبيعة التغيّر في المجتمع والسياسة.[١٦١] ويعتبرون أنّ تكنولوجيا المعلومات, هي مرحلة تطوّر, أكثر من كونها ثورة.

و يجد مؤيّدو ثورة المعلومات, الذين يرون فيها خيارات جديدة,أنفسهم أمام معارضين, يشدّدون أكثر على تهديداتها, ومخاطر تطبيقاتها. وبين الاثنين, هناك من يعتبر أن التطوّرات التكنولوجية, خلقت فرصا, وخلّفت تهديدات في نفس الوقت.

أما فئة المتحمّسين, فركّزت على الفرص التي نمت عالميا نتيجة الثورة التكنولوجية, والمجالات التي فتحت أمام لاعبين جدد, تمكّنوا من الوصول الى كافة ميادين المعلومات, ومن نشرها, مما أدى الى تمكينهم كقوّة في وجه الدولة. وفي نفس الوقت, حسّنت من فعالية الأجهزة الحكومية, وأدت الى تعاون وثيق بين المجتمع والدولة. وفي السياق نفسه, يدّعي كثيرون من منظّري وسياسيي عصر المعلومات, أن للإنترنت قدرة على الدمقرطة. حتى أن مفاهيم جديدة ظهرت كالتلديمقراطية 'teledemocracy', اي استخدام الانترنت لمشاركة مدنية أوسع في العملية الديمقراطية, نتيجة عوامل كثيرة كالقدرة على الوصول, والتوفر, والجذب, والقوننة, والتدفّق الحرّ للمعلومات, والسلوك البشري الذي هو متغيّر أساسي. وهناك من يرى أن عصر المعلومات, له أهمية عسكرية كبرى, نظرا لإمكانية تطبيق التطوّرات التكنولوجية على أنظمة التسلح, وجمع المعلومات, والمراقبة, ما خلق ساحة معركة جديدة, حيث التكنولوجيا تستخدم للحسم, والتأثير في تشكيل الأدراك, وخلق الآراء, والتحكّم في السلوك. حتى أنّ كثيرين من الأكاديميين, الأمريكيين منهم خاصة, ذهبوا الى القول, أنّ ثورة المعلومات عزّزت من عزيمتنا".[١٦٢]

أما المشكّكون, فشددّوا على التأثيرات السلبية لثورة المعلومات, مشيرين الى تعدّد المخاطر والتهديدات, التي تنشأ من تطبيقها على نطاق واسع, من أنشطة المجتمع . والبعض يتوقّع, أن يؤدي الإمتزاج بين التكنولوجيا والثقافة, الى تهديد الهوية.[١٦٣]

ويحذّر ***دافيد شانك David Shenk*** , من أن" تراكم المعلومات يهدّد قدرتنا على تثقيف ذواتنا, ويتركنا أكثر ضعفاً, ويحوّلنا الى مجتمع مستهلك, وأقل تماسكاً".[١٦٤] كما يطلق هؤلاء التحذيرات, حول العواقب

[161] Ibid, p:5

[162] Nye,J. 'Foreword', in Henry and Peartree (eds), The Information Revolution and International Security p. ix.

[163] OECD, 'Communiqué on Principles for Internet Policy-Making',p.7

العسكرية الناجمة عن تكنولوجيا المعلومات والاتصالات الحديثة, بحث يرفضون فكرة أنّ الحرب السيبرانية, أو الالكترونية, هي أقل عنفاً من الصراعات التقليدية . كما يعتبرون, أن التقارب بين التكنولوجيا العسكرية والمدنية, سيؤدي الى عسكرة المجتمع, وتحويل كل صراع, الى حرب سيبرانية.[١٦٥]

المطلب الثاني: قوةٌ سيبرانيةٌ متعدّدةُ المزايا

لقد أصبحت,المعلومات, بحسب الشروحات السائدة , مصدراً رئيسياً للقوّة. فمفهوم القوة الناعمة, يزعم أن "القوّة تنتقل من الغنى برأس المال الى الغنى في المعلومات."[١٦٦] ففي عصرٍ يتزايد فيه الترابط الاقتصادي, ويزداد تحرر السوق, تصبح الفئة التي تملك المعلومات, في موقع يعزّز من امتلاكها للقوة, مقابل ضعفا ينتابها, نتيجة تحدّي عدم التماثل.[١٦٧]

يعرّف ***كويل***, القوة السيبرانية, بأنّها " القدرة على إستخدام الفضاء السيبراني, لخلق منافع, وللتأثير في مجرى الأحداث, في كل البيئات التشغيلية,عبر أدوات القوة". ويقصد كويل بالبيئات التشغيلية, الميادين الخمسة للقوة (البرّ, والبحر, والجوّ, والفضاء الخارجي, والفضاء سيبراني), كما يقصد بأدوات القوة, أشكال القوّة الأربعة (الدبلوماسية, والمعلوماتية, والعسكرية, والاقتصادية). ويرى أن هذا التعريف للسيبرانية كقوّة, هو أوسع وأشمل من تعريفات أنواع القوّة الاخرى. فمثلا, هو أشمل من تعريف كلّ من ***آلان وستكوت ووليام ستيفانز William Stephens and Allan Westcott*** للقوّة البحرية, بأنّها "قدرة الدولة على فرض إرادتها على البحر".أو تعريف ***بيللي ميتشال Billy Mitchell***, وهو من روّاد سلاح الجوّ الأميركي, للقّوّة الجويّة, بأنّها" القدرة على فعل شيء في الجوّ", إذ أنّه يتضمّن, إشارة صريحة, لكلّ أشكال القوّة. كما أنّ هذا التعريف, يشدّد على أهمية تآزر وتكامل القوّة السيبرانية, مع أشكال وأدوات القوّة الأخرى.

ويضيف ***كويل,*** إنّ "القوّة السيبرانية هي قياس دائم للقدرة على استعمال البيئة التي يؤمنّها الفضاء السيبراني". وبرأيه إنّ للقوّة السيبرانية, دورا حيويا متزايدا في المجال الاقتصادي. ففي الثمانينيات من

---

[164] Shenk, D. (1997). Data Smog: Surviving the Info Glut. *Technology Review*, *100*(4),p. 15

[165] OECD, ‘Communiqué on Principles for Internet Policy–Making’,p.7

[166] Nye, ‘Soft Power’,p: 161

[167] Nye , J., & Owens, W. A. (1996). America's information edge. *Foreign affairs*, p. 20.

القرن الماضي, نشرت إدارة الرئيس الأميركي الأسبق رونالد ريغان, إستراتيجية أمنية قومية, لم تخل من الإشارة الى الدور الذي ستلعبه المعلومات, والتكنولوجيا الجديدة للمعلومات, في تقوية الإقتصاد الأميركي[١٦٨].

ويرى ***كويل,*** أنّ للقوة السيبرانية تأثيرا على العلاقات الدبلوماسية والسياسية , حيث الحملات المؤثّرة, التي تشنّها الحكومة الأمريكية, أو القاعدة,حيث يستخدم كلاهما هذه القوّة السيبرانية, للتأثير على العقول والقلوب. كذلك من الناحية العسكرية, حيث يعتبر أنها ربما تكون الأداة الأكثر تأثيراً, في العقدين الأخيرين, بدءا من "الثورة التقنية العسكرية" في روسيا في الثمانينيات, الى تطوير شبكة مركزية من المفاهيم, والتحوّل في السياسة الدفاعية للجيش الاميركي. فالفضاء السيبراني, والقوّة السيبرانية, كانا في صميم المفاهيم والنظريات الجديدة, من خلال مستويات النزاع, من التمرّد, الى الحروب التقليدية, بحيث أصبحت القوة السيبرانية, عنصرا لا غنى عنه, بالنسبة للقدرة العسكرية, المبنية على التكنولوجيا[١٦٩].

وقد ***رأى توماس فريدمان*** ***Thomas L. Friedma n*** في الفضاء السيبراني, عاملاً فائق الأهمية, في ربط جميع اللاعبين سوية في الإقتصاد العالمي للقرن الواحد والعشرين, والذي أسماه بإقتصاد "العالم المسطّح ***flat world***."[١٧٠].

أما ***شلدون,*** فيشير الى الفارق بين عبارتي الفضاء السيبراني والقوة السيبرانية, ويعتبر أن "الفضاء السيبراني, هو الميدان الذي تجري فيه العمليات السيبرانية". فبالنسبة له, إنّ "القوة السيبرانية هي مجموع المفاعيل الإستراتيجية التي تولّدها العمليات السيبرانية, في, ومن الفضاء السيبراني". هذه التأثيرات, يمكن تلمّسها ضمن الفضاء السيبراني, كما في الميادين الأخرى, من برّ, وبحر, وجوّ, وفضاء خارجي.[١٧١]

كما يرى في القوّة السيبرانيّة, ثلاث خصائص:

- أنّها حاضرة في كل مكان, مقارنة مع ميادين القوة الأخرى, قادرة أن تخلق تأثيرا استراتيجيا شاملا, في باقي الميادين, وفي الوقت عينه. ففي الوقت الذي يمكن للقوات البرية والبحرية والجوية, العودة الى الثكنات والموانئ والمرافئ, وحتى بما يتعلّق بالفضاء الخارجي, باستخدام الأقمار الصناعية الى هدف أخر,فإن القوة السيبرانية لا تعود الى مرسلها, ولا حدود لها.

---

[168] Kuehl. From cyberspace to cyberpower, p:11-12

[169] Ibid, p:13

[170] Friedman, T. L. (2005). *The world is flat: A brief history of the twenty-first century.* Macmillan.

[171] Sheldon. *Deciphering cyberpower* ,p:99

- مكمّلة لوسائل الضغط الأخرى, وهي لا تحدث أثرا مباشرا, وأنّ قوتها محدودة نسبيا. فالضرر الذي سببته دودة ستكسنت ***Stuxnet*** ,مثلا, لم يجبر القادة الايرانيين, على التخلّي عن برنامجهم النووي.
- هي قوّة خفيّة, فمن سمات هذه القوّة, جاذبيتها بالنسبة للكثيرين من مستخدميها, بحيث يمكن ممارستها خلسةً, وعلى نطاقٍ عالمي, دون أن تنسب الى الجاني. فالبرمجيات الخبيثة, يمكن زرعها في شبكات العدو, دون معرفة هذا الأخير بذلك, الى حين تفعيل هذا السلاح, وبالتالي التسبّب بالضرر المقصود. كما تمكّن المستخدم من مداهمة قواعد البيانات, للحصول على معلومات سريّة, أو خاصة, دون معرفة من أصحابها[١٧٢].

أما ***ناي***, فقد قدّم وصفا مختلفا للقوة السيبرانية, بقوله**:**" إنّ القوّة السيبرانيّة تعتمد على الموارد التي تميّز الفضاء السيبراني". ويرى أنّ القوة هي القدرة على تحقيق النتائج المتوخّاة, فالقوة السيبرانية, هي إمكانية القيام بالأمر نفسه في الفضاء السيبراني, أو هي إستخدام وسائل وأدوات الفضاء السيبراني, للحصول على النتائج المرجوّة, في الميادين الأخرى.[١٧٣]

ومن منظور ***كيفين باركر Kevin Parker***, للقوّة السيبرانية ميزات عديدة:

- **الانتشار العالمي**

عدد الاشخاص, والأماكن, وأنظمة الاتصال المتاحة في الفضاء السيبراني, هي في تزايد مطرد, مما يحسّن من القدرة العسكرية, في الوصول الى الأماكن والأنظمة, حول العالم. فالعمل في الفضاء السيبراني يؤمّن الوصول الى أماكن محظّرة على المجالات الأخرى. وقديماً ادعى مؤيّدو القوّة الجويّة, أن الطائرات استطاعت أن تتخطى حدود العدو, وتضرب مراكز قوة مباشرة في أرضه. اليوم, يؤمّن الفضاء السيبراني إمكانية الوصول الى مناطق متنازع عليها دون أن تعرّض العاملين فيها لأي خطر.

- **السرعة في التحرك والانتشار**

المعلومات تتحرّك في كابلات الألياف الضوئية بسرعة الضوء. كما أنّ مطلقي الهجمات السيبرانية, يمكنهم الحصول على تركيز أكبر لضرباتهم, بالإستعانة بكمبيوترات أخرى. فبتوزيع

[172] Ibid, p:99-100

[173] Nye, J. S. (2011). *The future of power*. PublicAffairs.

فيروس جاهز للعمل عند اعطائه الأمر بذلك, تطلق الآف الكبيوترات البوتنت, فورا ,هجوم تعطيل الخدمة, الذي يخلق حركة مرور مزيفة نحو موقع ما, معطلاً اياه.

- **الغموض**

مع تزايد أعداد المستخدمين للانترنت, أصبح من الصعب تعقب آثار أي مستخدم, فالغموض يتيح الحرية في الحركة, ويعيق إمكانية إسناد الفعل.

- **أفضلية المهاجم**

بالنسبة ***للكلوسويتزيين,*** إنّ القوة هي في الدفاع, اما في الفضاء السيبراني, فالأفضلية هي للمهاجم. فالمدافع يقف ضعيفا في وجه الهجمات المركزة, والسريعة, المستفيدة من الثغرات الأمنية لبعض الهياكل.

- **التمديد لطيف الأسلحة الغير قّتاكة**

إنّ الهجمات السيبرانية, تؤمّن استخدام وسائل غير قاتلة بوجه الخصم, فيبدوالأمر مغريا, ولكن الحماس يتدنّى عند إدراك محدودية ذلك, ومنها أن الخصم يمكنه ايضا أن يستخدم هذه الوسائل للرد, كما أنّ تأثير هذه الوسائل ضئيلٌ بالنسبة للخصوم, الغير متصلّين بالشبكات الالكترونية. فكلما إزداد الاعتماد على الفضاء السيبراني, كلّما ازداد الضعف أمام الهجمات السيبرانية.

- **تأثيرات من الدرجة الثانية**

قد تخلق الهجمات السيبرانية تأثيرات حركية, كإعطاء أوامر تدمّر أنظمة التحكّم الصناعية, ولكن لن تحدث الجراثيم الخبيثة انفجارا في أنابيب النفط, أو أن تغلق دودة كستاكسنت مثلاً مفاعلاً نووياً. [١٧٤]

---

174 Parker, K. L., & Force, U. A. (2014). The Utility of Cyberpower. *Military Review*, *94*(3), 26

أما ***بيتز وستيفنز Betz and Stevens***, فقد اعتمدا في تحليلهما للقوة السيبرانية,على تصنيف كلّ من ***بارنت ودوفال*** لمفهوم القوة,[175]حسب الآتي:

فقرة أولى: القوة الإلزامية

تكون عبر الإكراه المباشر, والممارس من قبل أحد اللاعبين في الفضاء السيبراني, في محاولة منه لتغيير سلوك وشروط وجود الآخر, أي إلزامه بالعمل وفق إرادته. والإكراه يمكن أن يمارس من قبل لاعبين من غير الدول. فالقوة السيبرانية الإلزمية, يمكن أن نجدها في التفاعل بين الدول, واللاعبين من غير الدول.فهناك أشكال من الصراع السيبراني تحدث غالبا, تكون الدولة فيها واحدة من لاعبين متعددين, متورّطين في هذا الصراع,كنشطاء, وقراصنة كمبيوتر, وإرهابيين, ومجرمين, ودول, وشركات خاصة وعامة وغيرها. فأي لاعب يمتلك المهارات والمعارف اللازمة, ولديه القدرة على الوصول الى الفضاء السيبراني, بمقدوره أن يمارس قوة سيبرانية إلزامية ضد الآخر. فمثلا,هجوم الأنونيموس الناجح, عبر الانترنت, على شركة ***HBGary Federal***, والتي تعمل على مكافحة البرامج الخبيثة, والحفاظ على أمن البيانات, برهن أنه يمكن للاعب من غير الدول, أن يمارس القوة السيبرانية الالزامية, تجاه الآخرين. فالشركة تعرّضت لهذا الهجوم, بعد كشفها الأسماء الحقيقية لأفراد هذه المجموعة, والمضمون الذي تنوي نشره, بعد تسلّلها الى موقعها على شبكة الانترنت, فما كان من هذه المجموعة, الاّ ان قرصنة خوادم الشركة,وشوّهت موقعها على الشبكة, وحمّلت عشرات الآلاف من رسائل البريد الالكتروني, ونشرتها على موقعها, كما قامت بمضايقة الرئيس التنفيذي, وغيره من موظفي الشركة, تاركة رسالة تهديد, في مؤتمر للأمن في سان فرنسيسكو, تسبّبت في عزوف الشركة عن إطلاق منتج جديد من البرمجيات, كانت ستعلن عنه في المؤتمر.

فقرة ثانية: القوة المؤسساتية

هي شكل آخر من أشكال القوة السيبرانية. ففي الفضاء السيبراني, يمكن إستخدام الموارد لوضع القواعد والمعايير للمؤسسات, للتأثير على سلوك المستخدمين. كما أنه يمكن استخدام هذا الفضاء, للتأثير على

[175] Betz & Stevens (2011) 46-51.

آراء الجمهور الأجنبي, من خلال وسائط الاعلام التابعة لهذه المؤسسات[١٧٦]. ففي السنوات الماضية, حاولت الولايات المتحدة الأمريكية, السيطرة على مؤسسة ***(ICANN).***[١٧٧]ورغم أنّ هذه المؤسسة تقدّم نفسها ك bottom–up كيان غير حكومي مركزه الولايات المتحدة, الاّ أنها تبقى تدور في فلك الحكومة الأميركية, وتحديدا, وزارة التجارة, التي تحاول التأثير في العمليات التي تقوم بها هذه المؤسسات, من أجل أهداف اقتصادية خاصة بها. وهذا مثال واضح, عن استخدام القوّة السيبرانية المؤسساتية. وفي عمل مشابه تشجّع الولايات المتحدة شكلا ناعما من "الردع السيبراني", من خلال مؤسسات عالمية متعدّدة عبر تشجيع والترويج للتغيير السلوكي والمعياري, لخارطة طريق للفضاء السيبراني.[١٧٨] ومع أن الكثيرين يتفقون مع موقف الولايات المتحدة, حيال هذه القضايا, الاّ أنّ هناك دولا لديها موقف مغاير, كالصين وروسيا تحديدا, اللتين تسعيان الى تفعيل قوتيهما السيبرانية المؤسّساتية, الخاصة بهما. فهما تمارسان هذه القوة, من خلال الاتحاد الدوليّ للاتصالات العالمي ***International Telecommunication Union (ITU)***, ومنظمة شنغهاي للتعاون ***Shanghai Cooperation Organisation (SCO)*** حيث تعزّزان من خلال هاتين المؤسستين, مصالحهما الوطنية, في مجال الحوكمة العالمية للإنترنت.

فقرة ثالثة: القوّة الهيكليّة

هي قوّة تسعى للحفاظ على الهيكلية, التي يوجد فيها اللاعبون الفاعلون , والتي تسمح أو تقيّد, الى حدّ كبير, الأفعال التي يرغبون القيام بها, تجاه الآخرين, والذين هم على اتصال مباشر بهم. ومن هذا المنطلق, تحدّد هذه القوّة, هيكلية تعامل الاشخاص مع بعضهم البعض. فالمبدأ التنافسي للرأسمالية, أعيد من خلال تحوّل بنى العمل المعرفي التعاوني والاتصالي بواسطة, والى حدّ بعيد, من الفضاء السيبراني, حيث تتوافّر السلع, والخدمات, وتستهلك, كما هي الحال في تحميل ملفات الموسيقى أو الأفلام, والخدمات المالية, والبيانات التجارية. ومع أنّ الرأسمالية قد تحولّت الى "مجتمع شبكات", الاّ أنّ المواقع

---

[176] Betz, D., & Stevens, T. (2011). *Cyberspace and the State: Toward a Strategy for Cyber-power*. IISS-The International Institute for Strategic Studies.p:.45-47

[177] The **Internet Corporation for Assigned Names and Numbers (ICANN**) is a nonprofit organization that is responsible for coordinating the maintenance and procedures of several databases related to the namespaces of the **Internet** – thereby ensuring the network's stable and secure operation

[178] http://moodle.oakland.k12.mi.us/os/mod/page/view.php?id=11722

البنويّة للرأسمال والعمل, ظلّت محفوظة, بقدر ما كانت خلال العصر الصناعي. لكنّ الشكل الشبكي أتى بجديد, فالشبكات المدنية المتمحورة حول أدوات الفضاء السيبراني, وفرصه, ومنتدياته, يمكنها الإلتفاف, وفي أوقات معيّنة, إستبدال الهياكل الهرمية للفترة الصناعية . فلشبكة الإنترنت, إمكانية تنظيم, وتحريك نشاطات المقاومة, بعيدا عن متناول الدول, وأجهزتها البيروقراطية البطيئة, وأنظمة السيطرة لديها. كأحداث الربيع العربي عام ٢٠١١, مثلا, والتي برهنت كيف أن للأنترنت قدرة على تحفيز, وتحريك المواطنين, وكيف أن الحكومات تحرّكت لقمع هذه النشاطات. فالقوة السيبرانية الهيكلية, تعمل على الحفاظ على, أو تعطيل الوضع القائم ***status quo,*** في آن معا.

فقرة رابعة: القوّة الإنتاجية

يشكّل الفضاء السيبراني بيئة معلومات نموذجية, وملائمة لأداء ونقل قوة سيبرانية منتجة. فالفضاء السيبراني, يهدف الى إعادة انتاج, وتعزيز الجدل القائم, وإعادة بناء ونشر نقاشات جديدة. فمن الأمثلة التي توضح, كيف تظهر الدول قوة سيبرانية منتجة, تصنيف لاعبين معينين كتهديد للأمن الوطني. وبناء على هذا التصنيف, تتّبع الدول سياسات واستراتيجيات, للتعامل معهم كأهداف مشروعة. فعبارة قرصان مثلا , تغيّر المعنى الذي كانت تحمله, في الخمسينيات وستينيات القرن الماضي, حيث أصبحت اليوم, تعكس صورة أفراد غير إجتماعيين , يشكلّون خطرا محتملا, ويعيثون فسادا في أنظمة الكمبيوتر, أكثر من كونهم "أبطالا" مسؤولين عن التجديد والإبتكار, في عالم الإنترنت . وفي حالات كثيرة, يعتبرون "العدو الجديد في عصر المعلومات.. واللاعبون السيئون في مجتمع الفضاء السيبراني". ورغم كون بعض القراصنة غير اجتماعيين ومدمرين, لكن كثيرين منهم, هم مجرد أشخاص معادين لنظام حكم معيّن, ويتصرفّون وفقا لذلك, كما هو الحال مع مسرّب الوثائق في ويكيليكس, ***جوليان أسانج Julian Assange***, والذي وضعت مجلة عالمية أخلاقه على المحكّ, واصفة إياه , بأنّه" صليبي, وقرصان, ومصاب بجنون العظمة, ومبتزّ."[١٧٩]

---

[179] Savage, L. **Julian Assange: The man who exposed the world** Crusader. Hacker. Megalomaniac. Extortionist. December 13, 2010 http://www2.macleans.ca/2010/12/13/a-man-of-many-secrets/.

وكما في أمور كثيرة متعلقة بالفضاء السيبراني, فإن هذه الثغرة لم يتم اصلاحها بعد, ومبادرات الحكومات الحالية ارتكزت على تقديم عروض وظائف[١٨٠], على من يسمون بالقراصنة الأخلاقيين ***ethical hacker,***[١٨١] عوضا عن التهديد بإعتقالهم. وفي السياق نفسه يطلق على هؤلاء في بريطانيا لقبا ملطّفا "الأولاد الأشقياء". ويشدّد بعض المعارضين, على ضرورة استبدال عبارة "قرصان اخلاقي" "بقرصان ذي قبعة بيضاء", وعبارة "قرصان غير أخلاقي" بعبارة "بقرصان ذي قبعة سوداء".[١٨٢]

على أنّ مقاربتي للقوة السيبرانية, كشفت من جملة ما كشفت, عن تغيير في مفهوم اللاعبين, ممن يمتلكون هذه القوة , ولو بدرجات متفاوتة, والأدوار التي يلعبونها. ويلاحظ في هذا السياق, وبشكل أساسيّ, تعددية اللاعبين, وتنوّع الوسائل التي يلجأون اليها, وخصوصية كلّ منهم, والأدوار التي يلعبونها على مستويات عدة, لا سيما لجهتي التعاون والتنافس.

---

180 http://www.usnews.com/news/business/articles/2016-03-02/pentagon-seeking-a-few-good-computer-hackers

181 القرصان الاخلاقي هو الشخص الذي يخترق شبكة الكمبيوتر لتفحص وتقييم سلامتها منعا من استغلالها من قبل القراصنة الخبيثين

182 Betz, D., & Stevens, T. 48-53

القسم الثاني:

لاعبو الفضاء السيبراني: تنافس غير متكافئ وتعاون محدود

شهد المجتمع الدوليّ, خلال العقد الأخير, انتشاراً لأنشطة غير سلمية في الفضاء السيبراني، تجاوزت الحدود الدولية، وفرضت تهديدات متصاعدة, نتيجة البيئة الأمنية الجديدة. فارتباط العالم المتزايد بالفضاء السيبراني, عمل على زيادة خطر تعرّض البنية التحتية الكونية للمعلومات لهجمات سيبرانية. الأمر الذي مكّن لاعبين من غير الدول من استخدام هذا الفضاء, لتحقيق أهدافهم, ما أثّر على سيادة الدولة. فانسحاب الدولة من قطاعات إستراتيجية لصالح القطاع الخاص وخاصة بالمنشآت الحيوية ، وتعامل الدول مع الشركات التكنولوجية المتعددة الجنسيات, والتي أصبحت تفوق قدراتها قدرات الدول, جعل من الفضاء السيبراني ساحةً جديدة لصراع, ذي طابع إلكتروني, يعكس النزاعات التي تخوضها الدول, واللاعبون من غير الدول, على خلفيات دينية, أو عرقية, أو إيديولوجية, أواقتصادية, أو سياسية. وتمدّد الصراع السيبراني بداخل شبكات الاتصال والمعلومات, متجاوزاً الحدود التقليدية وسيادة الدول، ومؤثّراً في امتداد مجاله وتداعياته أو آثاره.

ولأنّ الصراعات الدولية تستخدم شتى أنواع أسلحة التدمير الاقتصادية, والإلكترونية, والسياسية, والإعلامية، فإنها لم تتوان عن استخدام الفضاء السيبراني، بما له من قدرة على التأثير النفسيّ, والمعنويّ, والإعلاميّ, إضافة الى التأثير الأمنيّ, والعسكريّ, لتزحف جبهات القتال التقليدية, بشكل موازٍ لها إلى ساحة الفضاء السيبراني, فظهرت طرق بديلة عن الحرب المباشرة بين الدول, أو بين الخصوم, عبر شبكات الاتصال والمعلومات.

وإن كان إندلاع حرب سيبرانية مستقبلية, يعتبره البعض أمراً فيه الكثير من المبالغة والتهويل, فالتساؤلات تطرح حول ما إذا كانت الحرب السيبرانية, ضرباً من ضروب الخيال، أم هي بديلٌ من الحرب التقليدية. الاّ أنّه لا يمكن إنكار حقيقة أنّ الفضاء السيبراني سيغيّر من ميزان القوى العسكرية العالمية، وسيؤدي إلى تغيير جوهري في العلاقات السياسية بينها. وأنّ الحروب السيبرانية ستواكب الحروب التقليدية في المستقبل.

الفصل الأول: تعدّدية اللاعبين وتنوّع الاستخدمات

للفضاء السيبراني ميزات ساهمت في انتشاره, وزادت من الاعتماد عليه, وذلك لأسباب أسهبت في شرحها في فقرات سابقة, وأوجزها بما يلي: رخص التكلفة المادية, والسرعة في تبادل المعلومات, وسهولة الاستخدام, فضلا عن إمكانية تخفّي اللاعبين, وضعف قدرة الإسناد للأفعال السيبرانية. وهذا ما جعله بيئة جاذبة, ومجالاً للتوظيف في مجالات عدة من سياسية وإقتصادية, وإجتماعية, وعسكرية.

وعليه, تنوّع اللاعبون وازداد عددهم, ولم يعد يقتصر مجال استخدامه على تبادل المعلومات, بل أصبح بإمكان مستخدم ما أن يتسبّب في تعطيل شبكة البنى التحتية والاتصالات التابعة له, ملحقاً به خسائر فادحة اقتصادياً وعسكرياً, كقطع أنظمة الاتصال بين الوحدات العسكرية, أو تضليل معلوماتها, أو سرقة بياناتها السرية, أو مسح هذه البيانات. كل ذلك, بأسلحة لا تتعدى الكيلو بايتس, تنتشر بسرعة بين الكمبيوترات, وينطلق عملها بسرية تامة, وبكفاءة عالية, دون تمييز بين عسكري و مدني , أو بين رسمي وخاص.

ويرى ***ناي,*** أن الضرر في الفضاء السيبراني, يمكن أن ينجم عن أي أحد, بدءا من القرصان المراهق, الى الحكومة الحديثة. ففيروس "حشرة الحب", التي أطلقها قرصان فيليبيني, تسببّت بخسائر مالية بلغت ١٥ بليون دولار. كما أن شبكات الكمبيوتر التابعة للجيش الأميركي, تتم مهاجمتها الآف المرات يوميا. وقيل أنّ المجموعات الإجرامية, سرقت ما يقارب تريليون دولار من البيانات, والملكية الفكرية عام ٢٠٠٨. كذلك فإن شبكة تجسّس سيبرانية واحدة, قامت بأعمال تجسّس على ١٢٩٥ كمبيوتر, في ١٠٣ دول, ٣٠% منها أهداف حكومية. كما تستخدم الجماعات الإرهابية, الشبكة الالكترونية, لتوظيف أعضاء جدد, ولشن حملاتها.ويعمد الناشطون السياسيون, والبيئيون ,الى تخريب المواقع الالكترونية, للشركات والحكومات. ويضيف ***ناي,*** إنّ المصادر المتعددة للقوّة, التي يمتلكها مختلف اللاعبون, وضيق الهوّة بينهم وبين الدول, هي ما يميّز القوّة السيبرانية, عن غيرها في الميادين الأخرى .[١٨٣]

[183] Nye, The Future of Power, p:9

المبحث الأول: الدولة في الفضاء السيبراني: تحدٍّ للسيادة

كانت السيادة, ولا تزال, مادة إشكالية بامتياز. وقد طرأ على مفهومها تحوّلات جمّة من مطلق الى نسبيّ, وذلك ربطاً بالتطورات المتلاحقة (العولمة إحداها), وما أفرزته من معطيات جديدة (مسائل حقوق الانسان), وأملته من هياكل تنظيمية جديدة (الأمم المتحدة).

والتركيز على السيادة, ينطلق من اعتبارات عدّة, منها أن الدولة, لا تزال, وبنظر الكثيرين, ركيزة النظام الدوليّ, ليغوص في أشكالها من محلية, ومتبادلة, وقانونية, ووستفالية. ولكن آخرين يعتبرون أنّ الدولة لم تعد هى الفاعل الأول فى السياسة العالمية، حيث زاد تأثير الفاعلين من غير الدول، فاهتزت مكانة الدولة، وتحوّل الحديث من مبدأ سيادة وحرية الدول إلى سيادة وحرية الفرد داخل الدولة، وبدأت المنظّمات والشركات تطالب الدول بالتقيّد بقضايا كانت تعتبر فى السابق شأناً داخلياً، كالتركيز على مبادئ حقوق الإنسان ونشر الديمقراطية والحريات، خاصة حرية التملك والتعبير وتحرير التجارة. وقد واكب ذلك التراجع فى دور الدولة اكتساب الفاعلين من غير الدول أنماطا جديدة من التأثير والنفوذ.

على أنّ دراسة السيادة في الفضاء السيبراني, تتصل, من جملة ما تتصل, أولاً, بطبيعته, هل هو مشاع عام؟ مدوّراً بواقع الدولة فيه: هل هي قادرة على التعبير عن ذاتها, وممارسة وظائفها؟ أم هي مستباحة؟ وصولاً الى الشروط المطلوبة لتحقيق ذاتها, من دون إغفال التحدّيات التقنية التي تواجهها.

المطلب الأول: الدولة ركيزة النظام الدولي

لطالما شكّلت الدولة الركيزة الأساسية للنظام الدولي القائم, وهو أمر يعيده الأكاديميون الى سلم وستفاليا ١٦٤٨. فالدولة كانت تقليديا تشارك في الحروب, وتقيم التحالفات, وتعقد المعاهدات. أكثر من ذلك, إنّ المبدأ الاساسي لمنظمة الأمم المتحدة, هو أنّ المنظّمة قائمة على مبدأ المساواة في السيادة, بين جميع الدول الأعضاء.[١٨٤] فالحفاظ على سيادة الدول, هو هدف حيوي للمنظّمات الدولية, وللدول نفسها. فإبّان اجتياح العراق للكويت عام ١٩٩٠, أجاز مجلس الأمن الدولي استعمال القوة " لاستعادة السيادة,

[184] ميثاق الأمم المتحدة, المادة الثانية, الفقرة الأولى

والاستقلال, والحفاظ على سلامة أراضي الكويت".[185] وليس كلّ خرق للسيادة سيؤدي بالضرورة الى استخدام القوة, لكنّ الدول, تعتبر أنّ من حقّها الدفاع عن سيادتها. كذلك فإنّ الأمم المتحدة, غالبا ما تستخدم عبارة السيادة, بالتزامن مع الصيغة التقليدية للفقرة الرابعة, من المادة الثانية لميثاق الأمم المتحدة, التي جاء فيها: "يمتنع أعضاء الهيئة جميعاً, في علاقاتهم الدولية, عن التهديد باستعمال القوة, أو استخدامها ضد سلامة الأراضي, أو الاستقلال السياسي لأية دولة, أو على أي وجه آخر, لا يتفق ومقاصد الأمم المتحدة ". كما أنّ الكثير من قرارات مجلس الأمن الدولي, والجمعية العامة, المتعلّقة بالنزاعات بين الدول, تستخدم عبارة السيادة, وسلامة الأراضي, والاستقلال السياسي.[186]

ومن مظاهر سيادة الدول حقّها في ممارسة السيطرة الحصرية على أراضيها, وهذا الأمر, لا يتناسب برأي البعض, مع النقاشات الدائرة حول السيبرانية.[187] ***فغاري براون GARY D. BROWN*** يقول:"إني أجد الأمر مزعجا, عند سماع القادة العسكريين, يتحدّثون عن احتلال "الأرض العالية", أو يتفاوضون حول "الأرض السيبرانية", فقد تكون هذه اللغة مريحة لهم, لكن السيبرانية لا تقيم اعتبارا للجغرافيا ".[188] ويضيف, لطالما قدّرت حدود السيادة, بمساحة الأراضي التي يمكن للدولة أن تؤمّن لها الحماية. هذه هي حال الفضاء السيبراني اليوم. فالدول القوية في هذا المجال, ستعمل ما في وسعها للدّفاع عن البنى التحتية للإنترنت. كما أن الدول الضحية, غالبا, لا تعلم أنّ هذه البنى التابعة لها, تستخدم للتجسّس, أو كمسرح للعمليات للمجرمين السيبرانيين, أو للقراصنة, أو للاعبين من حكومات أجنبية. بمعنى آخر, السيادة السيبرانيّة, تمتد الى القدر الذي يمكن أن تصله الدولة.[189]

---

[185] S.C. Res. 661, U.N. Doc. S/RES/0661 (Aug. 6, 1990); see also S.C. Res. 674, U.N. Doc. S/RES/0674 (Oct. 29, 1990), and S.C. Res. 678, U.N. Doc. S/RES/0661 (Nov. 29, 1990)

[186] e.g., S.C. Res. 1680, U.N. Doc. S/RES/1680 (May 17, 2006) ; G.A. Res. 47/121, U.N. Doc. A/RES/47/121 (Dec. 18, 1992); S.C. Res. 1234, U.N. Doc. S/RES/1234 (Apr. 9, 1999)

[187] Jensen, E. T. (2015). Cyber sovereignty: The way ahead. *Tex. Int'l LJ*, *50*, 275.

[188] Brown, G. D. (2013). The Fourteenth Annual Sommerfeld Lecture-The Wrong Questions about Cyberspace. *Mil. L. Rev.*, *217*, p236

[189] المصدر نفسه,ص٢٣٨

وبرأي ***ناي***, أنّه طالما أن بنية الإنترنت التحتية هي جغرافية, وللحكومات سيادتها على مجالها الجغرافي, فالموقع, لا يزال يحتل حيزا من الأهمية, كمورد لها في الميدان السيبراني. فالحيّز الجغرافي يخدم كأساس للحكومات لتمارس الإكراه والسيطرة.[١٩٠] فعلى أعقاب أعمال الشغب في ***شينغيانغ*** في عام ٢٠٠٩, قامت الحكومة الصينية بحرمان ١٩ مليون مقيم, في مساحة بحجم مدينة ***تكساس*** الاميركية, من خدمة الرسائل القصيرة, والاتصالات الهاتفية العالمية, وخدمة الانترنت. الخسائر الناجمة عن ذلك طاولت عالم الأعمال والسياحة, لكنّ الإستقرار السياسي للبلد, هو ما أقلق الحكومة الصينية, وكان دافعها الأساسي لاتخاذ هذه الخطوة.[١٩١] وفي عام ٢٠١٠, فرض الإتحاد الأوروبي على شركة ***سويفت SWIFT***, المعنية بتحويل الأموال بين المصارف, وكنتاج لنقل خوادمها, من الولايات المتحدة الى أوروبا, وجوب الحصول على موافقة الاتحاد المسبقة, لعمليات الشركة الخاصة بتسليم الخزينة الأمريكية البيانات المتعلقة بمكافحة الإرهاب .[١٩٢]

كما يجادل ***ناي,*** أن الحكومات تستطيع أن تمارس قوة خارج نطاق أراضيها, لا سيّما اذا كان لها وجود في سوق أكبر , فمعايير الخصوصية الأوروبية, كان لها تأثير عالميّ. فعندما واجهت شركات مثل ***ياهو أو داو جونز Yahoo or Dow Jones*** , دعاوى قضائية تتعلّق بنشاط الإنترنت في فرنسا واستراليا, قرّرت الشركتان أن تمتثلا للحكومة, بدلا من الخروج من هذه الأسواق الكبرى. ويبدو أن هذا مصدر قوّة للحكومات التي تمتلك سلطة على الأسواق الكبرى, وليس بالضرورة الأمر نفسه للحكومات الأخرى.

كما يمكن للدول, وفقا ***لناي*** أن تشنّ هجمات سيبرانية عدائية, فمثلا, يشكّل الفضاء السيبراني ساحة قتال للأسطولين العاشر , والرابع والعشرين, من السلاح الجويّ الأمريكي.[١٩٣]

---

190 Nye, The Future of Power, P: 9

191 LaFraniere, Sh. and Ansfield, J.(2010), “Cyberspying Fears Help Fuel China’s Drive to Curb Internet,” New York Times http://query.nytimes.com/gst/fullpage.html?res=9C06E4DF1331F931A25751C0A9669D8B63&pagewanted=all

192 Pignal,S.(2010),“US presses Brussels on terror data swaps,” Financial Times, https://www.ft.com/content/99f8119e-1054-11df-841f-00144feab49a

193 Clarke, R. (2009). War from cyberspace. *The National Interest*, (104), 31-36 http://users.clas.ufl.edu/zselden/coursereading2011/Clarkecyber.pdf

المطلب الثاني: أشكال السيادة

يقدّم استاذ العلاقات الدولية, ***ستيفان كراسنر Stephen Krasner***, شرحاً عملياً ومفيداً, يمكن من خلاله فهم السيادة, وذلك من منطلقات أربعة :

- **السيادة المحلية:** تشير إلى الطريقة التي يتم بها تنظيم السلطة العامة داخل الدولة, ومدى قدرتها على ممارسة هذه السلطة بفعالية. فالسلطة السياسية سواء أكانت رئاسية, أم برلمانية, ذات نظام جمهوري, أو ملكي, ديمقراطية كانت أم سلطوية, تعمل على تنظيم وإدارة شؤونها الداخلية.
- **السيادة المتبادلة:** تتعلّق بإمكانية السلطة العامة, على مراقبة ما يتدفّق عبر حدودها, من أشخاص ومواد وأفكار. فعدم قدرة الدولة على تنظيم ما يمرّ عبر حدودها, سيؤدي حكما الى فشلها في السيطرة على ما يحدث في داخلها. وخسارة هذا النوع من السيادة, سيؤثّر في السيادة المحلية. فمناصرو العولمة, يجادلون في أنّ سلطة الدولة هي في تراجع, تجاه العديد من القضايا:كالتلوّث, والإرهاب مثلاً.
- **السيادة القانونية:** وتشير الى الاعتراف المتبادل بين الدول في النظام العالمي.
- **السيادة الوستفالية:** وتعني حق الدول في تحديد نظامها السياسي, ومنع اللاعبين الخارجيين, من التأثير في شؤونها الداخلية.[١٩٤]

ويذكر ***كرسنر***, أن هناك" حزمة من الميزات تترافق مع السيادة: كالإعتراف بها, ووحدتها, وقدرتها على بسط سلطتها".[١٩٥]ويبدو واضحا, أن تصنيف ***كراسنر*** للسيادة, بدا كعنصر مساهم في كشف زيف "أسطورة" عدم خضوع الفضاء السيبرانيّ, لسيادة الدولة. هذه "الأسطورة" مبنية على اعتقاد واسع, أنّ الفضاء السيبراني ليس بمكان ماديّ, وبالتالي يتحدّى القواعد التي تطبّق على الأرض, والبحر, والهواء, والفضاء الخارجي. ويبدو أن العمليات في الميدان السيبراني, تحدث خارج الدولة, في العالم الإفتراضي, لكن مفاعيلها تؤثّر على العالم الواقعي, داخل الدول. كما أنّ الفضاء السيبراني, يتطلّب بنى تحتية أرضية, تندرج في نطاق سيادة الدول.

---

194 Krasner, S. D. (1999). *Sovereignty: organized hypocrisy*. Princeton University Press.P 11-25 http://site.ebrary.com.ezproxy.aub.edu.lb/lib/aub/reader.action?docID=10031906

195 Krasner, S. D. (1999). *Sovereignty: organized hypocrisy*. Princeton University Press. http://site.ebrary.com.ezproxy.aub.edu.lb/lib/aub/reader.action?docID=10031906

المطلب الثالث: الفضاء السيبراني واختبار السيادة

بالعودة الى تصنيف ***كارسنر***, فالفضاء السيبراني يختبر السيادة المتبادلة, لأنّه يتحدّى قدرة الدولة على السيطرة على الحركة, عبر الحدود. فمع ترابط الفضاء السيبراني, يمكن لفرد في أفريقيا, أن يدخل الى الولايات المتحدة الاميركية, ويقوم بالعديد من الأنشطة الايجابية داخلها, كالتسوّق, والمراسلة, والحصول على تسجيلات الكترونية, وينجم عن ذلك نقل معلومات خارجها. كما يمكن للشخص نفسه, أن يدخل الولايات المتحدة, ويتورّط في أنشطة مؤذية, كقرصنة أنظمة الكمبيوتر التابعة للحكومة, أو تغيير رموز هذه الأجهزة, أو تعطيل الكمبيوتورات التي تشغّل هذه الأنظمة, كشركات الكهرباء العاملة داخل الولايات المتحدة الأميركية, على سبيل المثال. ولكن التحدّي الذي يشكّله الفضاء السيبراني للسيادة, لا يعني أن الدولة عاجزة عن ممارسة السيادة فيه. بل على العكس, فسيادة الدولة في الفضاء السيبراني, لا تتطلّب فقط الحصول على الاعتراف بذلك من قبل الدول الأخرى, بل ايضا أن تكون قادرة على ممارسة قدر من السيطرة على هذا الفضاء.[١٩٦]

وبالنسبة للسيادة المحلية, فقد أثّر الفضاء السيبراني على السلطة المحلية للدولة, وقدرتها على السيطرة, سواء أكان ذلك في ظل أنظمة الحكم الديمقراطية, أم الاستبدادية, حيث تحاول الدول التحكّم في وصول مواطنيها الى المعلومات, بذريعة أن محتوى بعضها, يشكل خطراً على الأمن القومي. أما التحدّي الأكبر للفضاء السيبرانيّ, هو بالنسبة للسيادة الوستفالية.[١٩٧]

ولقد كان لكلّ من الجيش من جهة, والأكاديميين من جهة أخرى, دور كبير في بدايات تطوّر الفضاء السيبراني. فكلّ منهما قدّم أفكاره حول كيفية تطوير. فالجيش أعطى الأولوية لمسائل "البقاء, والمرونة, والأداء العالي الكفاءة, على مسائل أخرى كانخفاض التكلفة, والبساطة, وجذب المستهلك". أما الأكاديميون, فقدّموا اعتباراتهم الخاصة ومنها " مركزية السلطة, والتبادل الحر للمعلومات". وبذلك, جمع الفضاء السيبراني معا ما أراده الجيش وما أراده الاكاديميون منه. لقد اعتبر الاكاديميون, أنّ "ازدياد تبادل المعلومات, يخلق مجتمعا أكثر تحررا, ويزيد من إمكانات التعاون. والتعاون المثالي, يحصد النتائج نفسها

---

[196] Franzese, P. W. (2009). Sovereignty in Cyberspace: Can it exist. *AFL rev.*, *64*, 1.p:8-9

[197] Liaropoulos, A. (2015). Exercising State Sovereignty in Cyberspace: An International Cyber--Order Under Construction? *Leading Issues in Cyber Warfare and Security: Cyber Warfare and Security*, *2*, 191

التي يعطيها التنافس المثالي, مع انتفاء وجود خاسرين"[198]. فالوصول الى هذا الهدف برأيهم, يتطلّب من الحكومات والشركات, عدم السيطرة على تكنولوجيا المعلومات, لأنّ كل من يسيطر على أنظمة المعلومات والاتصال, يسيطر على المحتوى المرسل أيضا. كما أعلن ***آبي هوفمان Abbie Hoffman***, في منتصف الستينيات من القرن الماضي: أن " حرية الاعلام, تنتمي الى هؤلاء الذين يملكون أنظمة التوزيع".

المطلب الرابع: الفضاء السيبراني مشاع عام!!

إنّ الاعتقاد أنّ الفضاء السيبراني يجب أن يتحرّر من تدخّل الحكومات, أدّى الى الإيمان بحصانته ازاء سيادة الدولة. وهذا ما يلخّصه كلام ***لجون باري بارلوJohn Perry Barlow*** , جاء فيه :" يا حكومات الدول الصناعية, يا عمالقة من لحم وصلب, أنا آت من الفضاء السيبراني, من منزل الفكر الجديد, اسأل الماضي, باسم المستقبل, أن يرحل ويتركنا بسلام. فلم يعد من المرحّب بكم بيننا. لا سيادة لديكم حيث نتجمع".[199] بالمقابل, يورد ***فرنزيس FRANZESE*** , خمسة أسباب, يدحض من خلالها حصانة الفضاء السيبراني, ازاء سيادة الدولة, كالآتي:

- إنّ استمرارية بعض الكيانات, تفرض ضرورة السيطرة على الفضاء السيبراني. فهذا الأخير يحتاج الى هيكل مادي, من دونه يفقد المستخدم القدرة على الوصول اليه. وهذا الهيكل المادي أرضي, ومن الطبيعي, أن يقع تحت سلطة الدولة حيث تتواجد المرتكزات المادية. كما أنّ الفضاء السيبرانيّ نفسه, يتطلّب التنظيم والمراقبة. فوجود ***شركة الإنترنت للأسماء والأرقام المخصصة***, وهي منظّمة مسؤولة عن التنسيق العالمي لنظام المعرفات الفريدة للإنترنت, وعن عملياتها الآمنة والمستقرة, تؤكد على أن الحاجة الى الرقابة ستزداد, مع ازدياد أعداد المستخدمين مستقبلا.
- إنّ العلاقات المالية في الفضاء السيبراني, تحتاج الى قوانين تنظّم تلك المعاملات, والعلاقات, والاّ كانت عرضة للمخاطر.

---

[198] Franzese, Sovereignty in Cyberspace: Can it exist, p;11

[199] Barlow, J. P. (1996). Cyberspace Independence Declaration http://www. eff. org/pub/Publications. *John_Perry_Barlow/barlow_0296. declaration.*

- إنّ المحتوى المرسل عبر الفضاء السيبراني, هو على قدر من الأهمية في العالم الواقعي. ففي الوقت الذي يتيح هذا الفضاء حرية تدفّق المعلومات , ليس هناك من استثناءات, فالدولة معنية بها, وهي التي تتلقاها وتحفظها.[٢٠٠] هناك مثلا مصلحة معلنة للولايات المتحدة الأميركية, ودول أخرى, في منع حيازة ونشر المواد الإباحية الخاصة بالاطفال. ولفرنسا مصلحة معلنة في منع انتشار التذكار النازي, ولاستراليا مصلحة معلنة في حماية مواطنيها من البيانات التشهيرية. وبالتالي فإن موقعا الكترونيا, يبيع التذكارات النازية من خارج فرنسا, والذي يمكن الولوج اليه من داخل فرنسا, يبقى خاضعا للقوانين الفرنسية.[٢٠١]
- إنّ الدول بحاجة دائمة لفرض حضورها في الفضاء السيبراني, نظراً لعلاقته بالأمن القومي. فالكثير من الدول تعمد, سواء عن قصد او عن إهمال, الى الاتصال, أو تشغيل الكثير من البنى التحتية الحيوية لديها, كالخدمات المصرفية والمالية, والنفط, والغاز, والكهرباء, والنقل, وسكك الحديد, والمياه, وغيرها, في أو عبر الفضاء السيبراني, ما يجعلها عرضة للاستهداف, بشكل متزايد.

إنّ النظرية الثانية التي ترى في الفضاء السيبراني, جزءا من "المشاع العالمي", تفتقد الى تعريف محدد لهذا المفهوم. فاستراتجية الدفاع القومي الاميركية, لعام ٢٠٠٨, لم تضع تعريفا محددا لهذا المشاع العالمي, بل أشارت اليه, على أنه المعلومات التي ترسل تحت المحيط, أو عبر الفضاء.[٢٠٢] ومعظم التعريفات, تركّز على الموارد الطبيعية, التي لا تخضع لسيطرة أمّة معينة. أمّا منظّمة الأمم المتحدة, ومنظّمة التعاون والتطوير الاقتصادية, (OECD) فتعرقّان "المشاع العالمي", بأنّه " الثروات الطبيعية, التي تقع خارج نطاق الولاية القومية, مثل المحيطات, والفضاء الخارجي, والانتركاتيك".[٢٠٣] لكن يتبيّن

---

200 Franzese,Sovereignty in Cyberspace: Can it exist,p;13

201 Goldsmith, J., & Wu, T. (2006). *Who controls the Internet?: illusions of a borderless world*. Oxford University Press.Goldsmith, Jack, and Wu, Tim. p147-161. ProQuest ebrary. Web. 9 October 2016.

202 U.S. DEP'T OF DEF. NATIONAL DEFENSE STRATEGY 16 (2008), available at http://www.defenselink.mil/news/2008/20national /20defense /20strategy.pdf.

203 Organization for Economic Co-operation and Development, Glossary of Statistical Terms, Global Commons, http://stats.oecd.org/glossary/detail.asp?ID=1 120 (last visited october. 8, 2016)

بعد التحليل, أنّ المحيطات, والفضاء الخارجي, ليست مشاعات عامة حسب هذا التعريف, وذلك للأسباب التالية:

- وجود معاهدات دوليّة تحكم كلّ من هذه الثروات الطبيعية. [٢٠٤]
- المعاهدات تحدّد ما يسمح به, وما يمنع, من استخدام هذه الثروات الطبيعية.[٢٠٥]
- تتناول المعاهدات, على وجه التحديد مسألة السيادة.[٢٠٦]
- تحدّد المعاهدات مناطق السيادة التي تشكّل المشاعات العالمية.[٢٠٧]

وعليه, إنّ الشرط الاساسي للمشاعات العالمية ليس المساحة التي تشكّل " الأماكن الطبيعية الخارجة عن نطاق الولاية الطبيعية". ويعدّد ***فرانزيس*** خمس خصائص للمشاع العالمي وهي :

- وجود اتفاقية دولية تحكمها.
- أن تحدّد هذه الاتفاقية ما هو مسموح وما هو ممنوع.
- المشاعات العالمية لديها حدود واضحة.

---

[204] اتفاقية الامم المتحدة حول قانون البحار والتي دخلت حيز التنفيذ عام ١٩٩٤, ووقعت عليها ١٦٧ دولة في ايلول ٢٠١٦

اتفاقية حول مبادئ حوكمة نشاطات الدول في اكتشاف واستخدام الفضاء الخارجي والتي دخلت حيز التنفيذ ١٩٦٧ بعضوية ١٠٤ دول

اتفاقية الانتركاتيك عام ١٩٥٩ والتي دخلت حيز التنفيذ ,١٩٦١ والتي وقعتها ١٢ دولة

[205] اتفاقية الانتركاتيك تحدد استخدامات الدول للانتركتيك لغايات سلمية كالابحاث العلمية, مثلا. وتمنع الدول من اجراء اختبارات الاسلحة النووية , أو التخلّص من النفايات النووية فيه. كما أن اتفاقية الفضاء الخارجي تسمح استخدام القمر وغيره من الأجرام السماوية لغايات سلمية بما فيها الابحاث العلمية, وتمع اطلاق اي سلاح نووي او سلاح دمار شامل فيه.اخيرا فان قانون البحار يتناول حقوق العبور, ووضع الكابلات البحرية ومد خطوط الأنابيب وحقوق الصيد ...الخ

[206] فاتفاقية الفضاء الخارجي, مثلا تنص على :"أن الفضاء الخارجي, بما في ذلك القمر, والأجرام السماوية الأخرى,غير خاضعة للاستيلاء , بإدعاء السيادة عليها ,من خلال الاستخدام ,او الاحتلال, او بأي وسيلة أخرى". كما أن قانون البحار, ينص على أنه" ليس لأي دولة, أن تخضع أي جزء من البحار لسيادتها, او ان تدعي, او تمارس السيادة على اي جزء من قاع البحر والمحيط, خارج حدود الولاية الوطنية". كما ان اتفاقية الانتركتيك تنص على " لا يجوز الادعاء بالسيادة في الانتركتيك خلال تطبيق المعاهدة"

[207] اتفاقية الانتركاتيك, تحدّد المشاع العالمي ب ٦٠ درجة الى الجنوب من خط العرض. كما اتفاقية البحار عددت ما لا يحصى من الأحكام التي تحدّد بدقة المناطق التي تشكل المياه الاقليمية. واتفاقية الفضاء الخارجي حددت المشاع العالمي بالقمر, والاجرام السماوية, مع غياب تعريف محدد للفضاء الخارجي في هذه الاتفاقية, وعدم وجود خط فاصل بين الفضاء الخارجي والأجواء الاقليمية.

- هناك اتفاق بين الدول, على عدم ادعاء السيادة الحصرية, فوق أي جزء من المشاعات العالمية.
- عدم قدرة دولة واحدة على التحكّم بالمشاعات العالمية.

بمعنى آخر, إن المشاعات العالمية, لا تعني غياب السيادة, بل وجود سيادة عالمية مشتركة. وبالتالي, إنّ تصنيف الفضاء السيبراني كمشاع عالمي, هو إشكالية بحد ذاته, لأنّ الخصائص المذكورة أعلاه, لا تتوافر في الفضاء السيبراني.[٢٠٨]

المطلب الخامس: إقرار بسيادة الدولة في الفضاء السيبراني

يعتبر ***ستيفن غورلي* STEPHEN K. GOURLEY,** أنّه يمكن تفسير السياسات المتخذة من قبل الدولة, للسيطرة على المعلومات التي تمر في المجال السيبراني, كشكل من أشكال ممارسة القوة, الأمر الذي يتوافق مع المفهوم الواقعي للسيادة, الذي يرى أنها سيطرة الدولة على إقليم معين, ضمن حدود هذه الدولة. و بناء على هذا المفهوم, فإن الدولة تمتلك وحدها الولاية, فارضة اياها من خلال مبدأي الإقليمية والآثار. فمبدأ الاقليمية يسمح للدولة بالتحكّم بالعمليات, التي تتم داخل وعبر حدودها, بينما يعطيها مبدأ الآثار, الولاية على النشاطات الخارجية, التي لها آثار داخلية. وهنا يكمن المعيار الأساسي لمفهوم السيطرة لدى الدولة. وبما أنّ المجال السيبراني هو بنى تحتية لها صلة بروابط جغرافية, ذات بناء من صنع الانسان, فكلّ عنصر يخضع لقوانين وولاية السلطة السيّدة, يجعل الأمر غير واضح بالنسبة للفضاء السيبراني. فالدول لم تعترف بعد بالسيادة في الفضاء السيبراني. فلكلّ منها سياسات وممارسات, تختلف عن غيرها, حيث يعتبر البعض أنّ الفضاء السيبراني هو من المشاعات العالمية (كالولايات المتحدة), في الوقت الذي لدى دول أخرى تصوّر مختلف لهذا الميدان, حيث ترى أنه يتطلّب السيطرة, للحد من تأثيراته وانعكاساته على السكان (كالصين). كذلك فإنّ الدول لا تتحكّم مباشرة بالفضاء السيبراني, أو بالنشاطات التي تحصل فيه. وقد يكون هذا نتيجة لعدم القدرة على إسناد الأفعال الى لاعبين محددين, فضلاً عن عدم وجود توافق في الآراء, بشأن ما يشكّل رد فعل معقول. فضعف الإسناد, يزيد من عدم التأكد من مدى صحة توجيه رد الفعل, اضافة الى إمكانية أن يكون هذا الرد, غير معقول أو غير متكافئ. أخيراً أنّ الكثير من الدول لا سيّما الديمقراطية منها, لم تستخلص بعد أنّ فرض السيادة

[208] Franzese, Sovereignty in Cyberspace: Can it exist, p;17-18

في الفضاء السيبراني, هو في صميم مصلحتها الوطنية, حيث تطلعات شعوبها الى الفضاء السيبراني أنه ذاك المجال الحر والمفتوح دون قيود. فالإستراتيجية الاميركية, التي لم تصرح ابدا عن سيادتها على الفضاء السيبراني, تعتمد سياسة مفتوحة آمنة في هذا المجال بأهداف محددة, بدافع أن الأمن السيبراني, وفي نهاية المطاف الأمن القومي, يعتمد على ما تضمنّه السيادة في الفضاء السيبراني حتى مع وجود نواحٍ أخرى, تعرض الامن القومي للخطر. فالنشاطات في الفضاء السيبراني, لها تأثير عالمي. وفي غياب الاتفاق عالميا على السيادة في الفضاء السيبراني, يكفي الاعتراف بسيادة فاعلة للدولة عليها, حيث تتواجد مكوناته, ما يتيح معالجة الآثار الفاعلة للسيادة, بينما يتم انتظار الحلول للتحدّيات التقنية والسياسية الناجمة عن تأسيس سيادة كاملة, وهي مسألة وقت وإرادة.[٢٠٩]

ولا بد من الاشارة الى ***دليل تالين***",[٢١٠] حيث وضع باحثون أمريكيون وأوروبيون, خلاصة منهجية, ومراجعة لتطبيق المبادئ المهمة في القانون الدولي التقليدي, ممثّلا بمبدأ السيادة في الفضاء السيبراني. والنقطة الاساسية هي, أنّ مبدأ السيادة يطبّق على فضاء الشبكة, معبرا عنه, " بأن الدولة, ضمن نطاق سيادتها, يمكن أن تفرض رقابة على البنى التحتية المعلوماتية, ونشاطاتها", حيث إنّ تعريف السيادة (بالاستناد الى حكم القانون الدولي, حول جزر البهاماس لعام ١٩٢٨),[٢١١] أكّد أنّ للدولة استقلالية في إدارة شؤونها الداخلية, دون تدخّل من الدول الأخرى, وعلى هذا الأساس, فللسيادة صلة بالفضاء السيبراني, فالبنى التحتية للمعلومات, بغض النظر عن مالكيها أو مستخدميها, هي تحت سلطة الولاية القضائية والإدارية للبلاد. وفي عام ٢٠١٥, ومن أجل تطوير المعلومات والإتصالات من منظور الأمن الدولي, قدّمت مجموعة من الخبراء الحكوميين, تقريرا للجمعية العامة للأمم المتحدة, أجمعت فيه, على أهمية ميثاق الامم المتحدة ومبدأ السيادة, الذي يشكّل أساس استخدام الأمن الالكتروني, وجاء فيه: " مع

---

209 Gourley, S. K. (2013). Cyber sovereignty. In *Conflict and Cooperation in Cyberspace: The Challenge to National Security* ,Taylor & Francis.p: 279-280

210 Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

211 Kirlin, J. P.(1926). REPORTS OF INTERNATIONAL ARBITRAL AWARDS RECUEIL DES SENTENCES ARBITRALES. *CONTRACT*, 162-163. http://legal.un.org/riaa/cases/vol_II/829-871.pdf (last visited 10,11,2016)

الاعتراف بالحاجة الى المزيد من الدراسة, لاحظت المجموعة الحق الطبيعي للدول في اتخاذ تدابير تتفق مع القانون الدولي, والمعترف بها في هذا الميثاق. [٢١٢]

المطلب السادس: من الدولة التقليدية الى دولة المعلومات

مثّل الفضاء السيبراني تحدياً على المستوى النظري والعملي للدولة, وساعد في ترسيخ فكرة أنّ الدولة لم تعد هي وحدة التحليل الأساسية, لرصد وتفسير الظواهر السياسية الدولية, وهي تواجه تحدّيات الحفاظ على سيادتها الارضية والسياسية , واحتكارها للقوة والنفوذ على النحو الذي أضاف مدلولات جديدة لوظيفة الدولة, وطبيعة دورها, في ظلّ صعود دور لاعبين من غير الدول, دخلوا في شراكة معها للقيام بوظائفها التقليدية. ويورد **عبد الصادق** النقاط التالية, في سياق تأكيده على تراجع الدور الوظيفي للدولة, وضعف سلطتها على إقليمها, والوظائف المنوطة بها:

- وجدت الدول نفسها أمام صعوبات, في فرض قيود على دخول البضائع اليها, وأمام القدرة على فرض الضرائب التي تشكّل أهم مورد من موارد الموازنة العامة للدولة, والتي تعبّر عن سيادتها بقدرتها على استخدام حقها المشروع في جني الضرائب, وبخاصة إذا ما تم تسريب رؤوس أموال محلية الى الخارج. وهذا يشكل ضررا اقتصاديا بالغا بالإستثمار المحلي, وأصبح بإمكان الشركات التكنولوجية الكبرى استخدام إعلانات تجارية للمنتجات, دون أن يتم دفع أي رسوم للدولة وهو ما يؤثّر على السوق المحليّة, ويعزز احتكارها للخدمات والتكنولوجيا بما يؤثّر على الاقتصاد الوطني.[٢١٣]
- إن الفضاء السيبراني قد أدّى الى تحوّل الدولة التقليدية الى دولة المعلومات التي تتسم بالتشبيك البنّاء, والمشاركة مع المواطنين, وتحتلّ الدولة في المنظور التقليدي, الدور المركزي بينما في

---

[212] Assembly, UN General. 2010. Report of the group of Governmental experts on developments in the field of information and telecommunications in the context of international security. A/65/201. http:// www.unidir.org/pdf/activites/pdf5-act483.pdf. (last visit:10,11,2016)

[213] عبد الصادق عادل. الفضاء الالكتروني والعلاقات الدولي: دراسة في النظرية والتطبيق, المكتبة الأكاديمية,٢٠١٦,ص١٧٧

دولة المعلومات أصبح المواطن هو المركز. وكانت الدولة التقليدية تتصرّف وفق رؤية نخبتها السياسية الحاكمة, بينما في دولة المعلومات برز لاعبون جدد في المجال العالمي, وأصبح لديهم القدرة على التأثير في السياسيات العامة. وتتميّز الدولة في ظل الفضاء السيبراني بقدرتها على امتلاك أساليب عمل مرنة وسريعة الاستجابة, وتعتمد على رأس المال الفكري, كما أنّ معدّل استجابتها للمواطنين أصبح يقاس بالساعات بدلا من الشهور.

- أتاح الفضاء السبراني الفرصة لإحداث تغييرات في مجال وظائف الدولة, وبخاصة فيما يتعلق بوظيفة الدفاع الخارجي, والمتمثّلة في السلطة الفعلية في المؤسسة العسكرية, التي تتعلّق بسلامة الدولة وأفرادها, من العدوان الخارجي. كما ساهم في وجود أشكال جديدة من العدوان على مواطني الدولة ومؤسساتها, عبر شبكات الإتصال والمعلومات, والتي تعتمد عليها المنشآت الحيوية, وهو ما يصيب الدولة بعجز في توفير الأمن على المستوى الداخلي, بحفظ سلامة الأفراد وممتلكاتهم وأموالهم, وكذلك مهمة الدفاع, لعدم القدرة على تحديد مصدر الهجمات ومن ثم أخذ رد فعل سريع . كما ساعد الفضاء السيبراني في دعم الحركات الانفصالية في مواجهة الدولة, وفي التأثير على الهوية القومية.
- لم تستطع الدولة الحفاظ على تراثها الثقافي لشعبها مع ما يحمله الفضاء السيبراني من تأثيرات لقيم وثقافات خارجية مهيمنة, في تشكيل تحدي للثقافة المحلية. كما أثّر على حق الدولة السيادي غير القابل للتصرف في تقرير نظامها السياسي والاقتصادي والثقافي والاجتماعي بحرية, وفي تنمية علاقاتها الدولية وفي ممارسة سيادتها الدائمة على مواردها الطبيعية, وفقا لإرادة شعبها, دون تدخّل, أو تداخل, أو تخريب, او تهديد من الخارج بأي شكل من الشكال.
- أدّى الفضاء السيبراني الى تعاظم أزمة الدولة القومية, وأصبح من الصعب اعتبارها لاعبا رئيسيا في العلاقات الدولية, وهو ما أدّى الى انفتاح علاقات بين المجتمعات, على مستويات مختلفة دون الدولة.[٢١٤]

لكن, من جهة أخرى, نشّط الفضاء السيبراني المجتمعات المحلية, وزاد الروابط بين الأفراد والمجتمع, حيث زادت الحالة التفاعلية بين الأفراد, سواء أكان في شكل فردي, أو في شكل تنظيمات سياسية وحركات اجتماعية, والتي تدعو الى الحكم الديمقراطي, والعمل على بناء هويات فاعلة, تسعى لأن يكون

[214] المصدر نفسه ص: ١٧٨-١٨٠

لها دور في اللعبة السياسية, مع زيادة الوعي بالهويّات المحليّة وأهمية دورها في العملية السياسية. كما أمّنت الإنترنت للحكومات امكانية التواصل المحلي مع المواطنين دون وسطاء حكوميين, مما أدّى الى الوصول الى درجة من الرضى عن آدائها. كما فعّل آليات الحوار مع اعضاء الحكومة السياسيين و مع القاعدة الحزبية او الجماهيرية.

المطلب السابع: استباحة السيادة

إنّ السيادة الإقليميَّة, أصبحت مفتوحة ومستباحة بفضل التقدم التكنولوجي، وأصبح الأقوى تكنولوجيا يتمتّع بقدرة فائقة على اكتشاف ما يجري عند الآخرين, ومعرفة أدقّ أسرارهم من دون استئذانهم. ويذكر على سبيل المثال, عمليات التنصّت أو استراق السمع, والتجسّس؛ والتقاط الصور بواسطة الأقمار الصناعيّة . والخطورة في مثل هذه التصرّفات لا تَكمن في إفراغ السيادة من مضمونها, أو فاعليتها فقط، بل تكمن أيضا, وأساسا, في أنّها لا تعدُ خرقا لقواعد القانون الدولي العام.

فالتطوّرات العلميّة التي تَسمح باستخدام الفضاء السيبراني، وبعُبور شبكة الاتّصالات الوطنيّة أحيانا، تَجعل من الصعب، عمليًا، ممارسة السيادة الوطنيّة على هذا المجال السيبراني، وإخضاعه, أو إخضاع أيّ جزء منه للتشريعات, أو المراقبة المحليّة. ونظرا لصعوبة الرقابة, أو استحالة تحديد أماكن إنتاج برامج المعلوماتيّة التي تسير في الفضاء السيبراني, وتنتقل من دولة إلى أُخرى بسرعة هائلة، فإنّ الدول لم تبد، منذ أن غزت البرامج المعلوماتيّة المجال السيبراني، أيّ اعتراض أو احتجاج, على تغلغل هذه البرامج في إقليمها. ولهذا تخلّت معظم الدول عن التشبّث بفكرة السيادة".[٢١٥]

ويورد د. ***طارق المجذوب***, سلسلة من التحديات, التي واجهت هذه الدولة بفعل التقدم التقني, في مجال الفضاء السيبراني:

- **تحدٍّ إقتصادي سياسي,** نتج عن تعميم تكنولوجيا المعلومات لأسلوب الاعتماد المتبادل بين الدول, وشركات تكنولوجيا المعلومات متعدّدة الجنسيّة, والذي يعني أنّه لم يَعُد في مقدور أية

[215] **السَّايْبِر ساحة "خَفِيَّة" لحربٍ "ناعِمَة" قادِمة!** https://www.lebarmy.gov.lb/ar/content – العدد ٨٩ تموز ٢٠١٤

دولة, الاعتماد على الذات فقط، والاكتفاء بما تنتج من منتجات المعلوماتيّة. وهذا الوضع, حتّم على الدولة الاستعانة بغيرها من شركات تكنولوجيا المعلومات، أو الاعتماد على غيرها، لسدّ حاجاتها العسكريّة. فتقدّم صناعة برامج المعلوماتيّة, فرض على الدولة توسيع دائرة اتصالاتها الخارجيّة, والدخول في أنماط جديدة من الشراكة مع القطاع الخاص,بعد أن كانت الدولة تتحكّم وحدها في آلة صنع القرار السياسي, وهذا الأمر كان ممكنا قبل ظهور تكنولوجيا المعلومات التي أصبحت تتطلّب قدرا كبيرا من الاختصاص والمهارة والخبرة والتفرّغ، وإلماما واسعا بالأجهزة الإلكترونيّة المتطوّرة، ومعرفة عميقة بالمعلوماتيّة وثورة الاتصالات. أصبح من الصعب اليوم على أجهزة الدولة وهيئاتها, إدراك مختلف أَبعاد صناعة برامج المعلوماتيّة واستيعاب جميع ظروفها وتطوّراتها. وبذلك أصبح لزاما عليها اللجوء إلى المتخصّصين والمؤهّلين من شركات تكنولوجيا المعلومات. فالتطوّر العلمي في مجال صناعة برامج الكمبيوتر أفضى بفعل التَّعقيدات التي أَفرزها، إلى تراجع دور الدولة التقليدي في المجال العسكري وتصاعد دور شركات الصناعات الحربيّة:

- **تحدّي السيطرة على ثورة الاتّصالات** وموجاتها المختلفة (التحدِي الرقمي، مثلا). فالدولة كانت, قبل انتشار استخدام الفضاء السيبراني، قادِرة على تحديد تدفّق المعلومات وتغلغلها، بشكل نسبي مقبول.غير أنّها أصبحت، بعد انتشار البرامج المعلوماتيّة، عاجزة عن التحكّم الكامل بسيلها. فكيف باستطاعة الدولة, منع سرقة المعلومات الإلكترونيّة وتعديلها وإعادتها إلى حيث سرقت؟ وهل بإمكانها عمليا منع الخاطفين أو القراصنة المحتملين, من التقاط ما تنقله برامج الكمبيوتر من معلومات ومشاهد؟ وهل بإمكانها عمليا منع التنصّت أو استراق السمع، أو انتهاك سريّة المراسلات والاتّصالات، أو اعتراض أو اختراق ما تبثُه البرامج الخبيثة من معلومات ومشاهد؟
- **تحدٍّ أمني** لكون الفضاء السيبراني قد غيّر أنماط العلاقات الدولية وقواعد الحرب. وبنتيجة ذلك, لم يعد للحدود حرمة أو أهميّة، ولم يَعُد خطر التدمير محليّا يقتصر على أطراف النزاع, بل يمكن أنْ يمتد إلى دول عَبَرت شبكاتها الوطنيّة البرامج المعلوماتيّة الخبيثة .

ويتابع د. ***المجذوب***, إنّ تطوّر وسائل الاتصالات ووسائطها ساهَم في زعزعة الوظيفة التوجيهيّة للدولة, في كل ما يتعلّق بالتحكّم بالفضاء السيبراني, بحيث أضحى مفهوم الحدود السياسيّة والجغرافيّة، وكذلك مفهوم السيادة ومفهوم الاستقلال عن الآخرين، من المفاهيم الغابِرة التي لا يمكن الاعتداد بها. [216]

المطلب الثامن: منافسة الفرد للدولة

ارتبطت قوّة الدولة تقليديا بعدة عوامل أهمها:

- امتلاك المعلومات واحتكارها, ضمن منظومة بيروقراطية, تمكنها من ممارسة ادوار مؤثرة على تدفق المعلومات ومضامينها كالتعتيم, والاجتزاء, والتحريف, والتحكم بآليات النشر.
- توّفر ما يكفي من أدوات الرقابة, التي تتيح لها إدارة المعلومات, بما يتوافق مع مصالحها واهدافها.
- احتكار أدوات القمع, التي تسمح ببسط سيطرتها على الفضاء السيبراني والتحكم بسلوك الافراد داخله, مستفيدة من قدراتها التقنية, وقدرتها على التشريع وسن القوانين.

في المقابل, ترتبط قوة الفرد كلاعب في الفضاء السيبراني, في مجال انتاج المعلومات وتداولها في الفضاء السيبراني بما يلي:

- النمو المطرد للفضاء السيبراني, والذي يتم بوتيرة أعلى من تطوّر أجهزة الرقابة, الأمر الذي من شأنه توسيع مجال الحريات.
- انخفاض تكاليف انتاج المعلومات ونقلها وهذا يعطي الفرد العادي موقعا تنافسيا في مواجهة الموقع الاحتكاري التقليدي الذي تمتلكه الحكومات والشركات الكبرى, في مجال الاعلام والاتصال.
- الاعتقاد السائد, أن الفضاء السيبراني أثّر على توازن القوى بين السلطة والفرد, لصالح هذا الأخير, لأسباب عدة تلخّص كالتالي:

---

[216] المصدر نفسه

- زيادة أعداد الفاعلين القادرين على تجاوز الموانع الاقتصادية والسلطوية والقانونية, في ظل تآكل نظم الرقابة, والكلفة الزهيدة للمشاركة التفاعلية, في الشبكة العنكبوتية.
- فتح مسارات جديدة للعمل السياسي, تتخطّى الحدود الجغرافية والأطر التقليدية وهذا يزيد من فعالية بعض الفئات المهمشة, كالشباب الذين سجلوا حضورا مفاجئا خلال الانتفاضات الجماهيرية في مصر وتونس مثلا.[٢١٧]

هناك إذن تحولاّت مؤثّرة, عزّزت حضور الفرد وقوته في وجه السلطات المقابلة له (دولة, جماعات, طوائف, عشائر..) الى حدّ القول, حسب تعبير ***جيرمي ريفكن Jeremy Rifken*** بأنّ ثورة المعلومات ساهمت في كسر المفاهيم التقليدية للمجتمع, والذي تحوّل معناه من مجموعة أفراد مع تاريخ وثقافة مشتركين الى مجتمع افتراضي. والعالم الافتراضي الذي لا تفصل حدود مادية بين شعوبه يبعث على الإعتقاد حسب ***ريفكن*** ايضا, بأنّ الدولة الأمة لن تقوى على الصمود على الأقل في صيغتها الراهنة.[٢١٨]

ومع التسليم بصحة ما ورد من تحوّلات أفضت الى تعظيم دور الفرد, في مقابل السلطة, إلا أنّ تعظيم هذا الدور, لن يكون بالضرورة على حساب نفوذ الدولة. بل تبرز قوّة الدولة في الفضاء السيبراني من خلال الاتي:

- ما زالت الدولة حتى الآن اللاعب الرئيسي في مجال فرض الأمن, على صعد عدّة, بما فيها الأمن السيبراني, كما أنّها المستثمر الرئيسي في البنى التحتية الرقمية, وهي التي تضع قواعد تنظيم البيانات والمعلومات والضامن الأخير لاستمرارية تدفّقها.
- فقدت الدولة بعض قدراتها الرقابية مع التطوّر المطرّد لتقنيات المعلومات, لكنّ ذلك لم يزد مساحة الحرية, بل انتقلت سلطة الرقابة من الداخل الى الخارج, فصارت الدول التي تتحكّم بشبكات المعلومات, كالولايات المتحدة الاميركية, والشركات الكبرى المشغلة للفضاء السيبراني, كموقع ***فيسبوك*** قادرة على الحجب والاتاحة, بناء على السياسات العامة التي تعتمدها وتفرضها على الآخرين, واستنادا الى البروتوكولات الموضوعة غالبا من طرف واحد.

---

[217] فضل الله عبد الحليم, علاقة المواطن بالسلطة في العصر الرقمي, المركز الاستشاري للدراسات والتوثيق ٥-١١-٢٠١٣ ص ٤-٥

[218] Rifkin, J. (2000). The age of access: The new culture of hypercapitalism. *Where All of Life is a Paid-For Experience, Tarcher, New York*, *33*, 40-51.

- في الوقت الذي تتآكل فيه الرقابة نسبيا, تزيد قدرة السلطات على خرق الخصوصية, وجمع المعلومات عن الأفراد, وتعقبهم وتتبع آثارهم. فالتطوّر المتسارع لتقنيات المعالجة والتخزين والتحليل الرقمي, يؤدي في نهاية المطاف الى كشف باطن المجتمع وزيادة هشاشته.
- في عصر الثورة التقنية تتراجع ولا شك قدرة الحكومات على التحكّم بتدفّق المعلومات أو الحفاظ على السرية, لكنّ قدرتها لا تتراجع في ميدانين:

  - التحكّم بانتاج المعلومات, الذي يتطلّب استثمارات كبيرة,على عكس الكلفة الزهيدة لتداول المعلومات أو إعادة انتاجها. إذ بوسع الحكومات أن تستثمر في مجالات وتهمل أخرى لأسباب تتعلّق بمصالحها.
  - بوسع السلطات أن تستفيد من شبكات المعلومات للدعاية, وتحوير الحقائق, والتضليل, دفاعا عن سلوكها وسياساتها، بل يمكنها أيضا التعاون مع الشركات لإنتاج تطبيقات برمجية مقيدة للحريات.[٢١٩]

ويميّز ***وليام دريك William Drake*** بين نوعين من السيادة : السيادة الدستورية لدولة ما على أراضيها من جهة, والسيادة العملانية, التي تعني فعالية الدولة في الإشراف والرقابة على أراضيها. وبرأي ***دريك***, النوع الأول من السيادة لا تشكل ثورة المعلومات تحديا له لأنه محميّ بالقوانين, والمعاهدات, والمواثيق الدولية, ولكن النوع الثاني من السيادة, هو الذي تهدّده المعلوماتية, تقنيا ولجهة التكلفة كذلك. كما أن السيادة السياسية, أي قدرة الدولة على اتخاذ قرارتها بنفسها, وداخل حدودها, تتعرّض بدورها للتهديد في ظل العولمة. بالمقابل, هناك من يقلّل من شأن تقلّص السيادة القومية من هؤلاء ***بول براكن Paul Bracken*** الذي توقع تصاعد القومية, ولا سيما في آسيا, أي زيادة قدرة الدولة على التحكّم في مجالها السيادي مع امكانية تراجعها في الدول المتقدمة, حيث يرى الكاتب ايضا أنّ عصر المعلومات يؤدي الى تدمير متسارع يتسبّب في اختلالات في الأمن السياسي والاجتماعي والشخصي. وخصوصا لدى أبناء الطبقة الوسطى. ولكن هذا الأمر يمكن أن يؤدي الى زيادة دور الدولة لا تراجعها, بحكم أنها الضامن

---

219 فضل الله, علاقة المواطن بالسلطة في العصر الرقمي, ص ٧–٨

الأكبر للأمن الشامل. لكن الدولة ذات السيادة, بوسعها أن تؤدي ايضا دورا تحريفيا, عندما تتحوّل الى مصفاة تكرير المعلومات التي تصير أكثر تعبيرا عن وجهة نظرها لا عن الحقائق.[٢٢٠]

المطلب التاسع: شروط تحقّق السيادة في الفضاء السيبراني

قبل تحقّق السيادة في الفضاء السيبراني, لا بدّ للدول أن تراعي نقاطا أربعا, وهي:

فقرة أولى: الإعتراف بالفضاء السيبراني كمجال سيادي

يكون ذلك عبر اقتناع الدول أنّه ميدان يمكن للدولة أن تمارس سيادتها عليه, ومن ثمّ اتخاذ خطوات إضافية لرسم معالمه, ليسهّل عليها ممارسة السيادة عليه. فبالرغم من أن وزارة الدفاع الأميركية, مثلا, وقّعت الاستراتيجية القومية العسكرية للعمليات في الفضاء السيبراني, والتي تنصّ على أنّه ميدان خاص بها, جنب الى جنب مع الميادين الأخرى, البرية, والبحرية, والجوية, والفضائية[٢٢١], فإنّ التعامل معه, كميدان منفصل, لا يخلو من الجدل. حتى إنّ البعض في وزارة الدفاع الاميركية, يعتقدون أنّه لا يشكّل مجالاً بحدّ ذاته.[٢٢٢] فهذا الجدل, لا يمنع الحقيقة الأساسية, أنّ الفضاء السيبراني هو من صنع الانسان, وأنّ الدول تمارس سلطة عليه. فوجوده يتطّلب هندسة مادية وبحاجة الى قوننة, لكي يعمل بفاعلية, والدول تحاول زيادة التحكّم في هذا الميدان.[٢٢٣]

---

220 Hundley, R. O., Anderson, R. H., Bikson, T. K., Dewar, J. A., & Green, J. (2000). *The Global Course of the Information Revolution: Political, Economic, and Social Consequences Proceedings of an International Conference*. RAND NATIONAL DEFENSE RESEARCH INST SANTA MONICA CA.

221 http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf (last visited 16,10,2016)

222 Luber, D. R., & Wilkinson, D. H. (2009). Defining Cyberspace for Military Operations. *Marine Corps Gazette*, *93*(2), 40.

223 Franzese, Sovereignty in Cyberspace: Can it exist, p:34

فقرة ثانية: طلب السيادة في الفضاء السيبراني

بالرغم من الإعتراف بالفضاء السيبراني, كمجال يمكن للدول أن تمارس سيادتها عليه, يبقى السؤال الأهم, هو ما اذا كان هناك رغبة لدى الدول, بفرض سيادتها عليه. فصيانة السيادة, يتطلّب في نهاية المطاف, نظاما دوليا محدّد القواعد والاجراءات التي تنظّم نشاط الدولة في هذا المجال, بما في ذلك ضرورة تحديد وتعقّب الفاعلين العبر دوليين. فقد تعارض بعض الدول السيادة في الفضاء السيبراني, والرقابة الدولية التي تنتج عن ذلك, بالإشارة الى دوافع الولايات المتحدة الاميركية والصين, مثلا. وقد يصبح الفضاء السيبراني, ميدانا يمكّن الولايات المتحدة الاميركية, من نشر قيمها الديمقراطية, والترويج لمثلها وأفكارها. كما ورد في الاستراتيجية الأمنية القومية الاميركية لعام ٢٠٠٦[٢٢٤]. فسعيها لضمان حرية التعبير, و تبادل الأفكار, كوسيلة لنشر الحرية, يمكن تحقيقه بشكل غير مباشر, من خلال تطوير شبكة إنترنت حرة ومفتوحة. وفي حين أنّ هذه وجهة نظر مثالية, فإنّ الادلّة متزايدة على أنّ تأثير الانترنت, يعزّز مصالح الولايات المتحدة. فعلى سبيل المثال, لقد غيّرت الإنترنت من التفاعل بين الدولة الصينية والمجتمع, من خلال تقويض احتكار النظام الشيوعي (لتقنيات وسائل الاتصال والمعلومات), والسماح في توفير مساحة عامة للمدنيين, للمشاركة في الحياة السياسية, وفقدان الثقة العامة في مؤسسات الدولة. وهذا يتماشى, الى حد ما, مع استراتيجة الامن القومي الاميركية.[٢٢٥] وتأتي إيران, في عداد الدول التي ترغب الولايات المتحدة الاميركية في التأثير عليها ايجابيا من خلال الفضاء السيبراني. ففي عام ٢٠٠٠, ازداد اعتماد الايرانيين على شبكة الانترنت للحصول على الاخبار والاراء.[٢٢٦] ولعبت الإنترنت دورا في تنظيم الاعتراضات في ايران, بعد الجدل الواسع الذي تسببّت به الإنتخابات الرئاسية, في حزيران ٢٠٠٩. اذاً بوجود إنترنت حرّة ومفتوحة, تسهّل انتشار أهداف الولايات المتحدة, في نشر الديمقراطية والحرية, يمكن لوجود نظام دولي حول السيادة في الفضاء السيبراني, أن يؤمّن للدول فرصا وامكانيات أكبر, للتحكّم في الخطابات والمعلومات التي تنتشر, من خلال السماح للدول, بمراقبة اللاعبين والمحتوى الذي

---

224 Bush, G. W. (2006). *The national security strategy of the United States of America*. Wordclay.p:9 https://www.comw.org/qdr/fulltext/nss2006.pdf

225 Ibid,p:186

226 Memarian O.(Dec. 9, 2005)Internet Yearns to Be Free in Iran, SAN FRANcISco CHRON. http://www.sfgate.com/opinion/openforum/article/International-Human-Rights-Day-Internet-yearns-2590171.php

ينشر, عن كثب. كذلك قد تعارض الولايات المتحدة, سيادة الدول على الفضاء السيبراني, لأنها تتصّب نفسها المسيطر على القوّة السيبرانيّة, التي تتجم من فضاء سيبراني متحرّر من سيادة الدول. من ناحية أخرى, فقد تفرض السيادة في الفضاء السيبراني, درجة من الانفتاح, قد لا ترغب فيه الصين. ذلك أنّ تطوير السيادة على هذا الفضاء, تتطلّب قواعد واجراءات متفق عليها, كمتى, وما نوع المحتوى والمعلومات, التي يمكن أن تمرّ من خلال هذا الفضاء, وعبر الحدود, ومباشرة الى المواطنين في كل دولة. كما تنص المادة ١٩ من الاعلان العالمي لحقوق الانسان, حول الحق في حرية الرأي والتعبير. وهذا الحق يشمل الحرية في اعتناق الاراء, بدون تدخل بأية وسيلة, ودون أي اعتبار للحدود. لذلك, فإنّ أي نظام دولي حول الفضاء السيبراني, سيتضمّن هذه القيم, وهذا ما تعارضه الصين.[٢٢٧] كما أن كلا البلدين, الولايات المتحدة والصين, يفضّلان فضاء سيبرانيا بلا سيادة حاليا, لأن هذا الفضاء هو في نموّ مطرد, وبالتالي, فالدول تفضل الانتظار, قبل الدخول في اتفاقات, تحدّد النشاطات الممنوعة والمسموحة, ريثما تتعمّق في فهم أكثر للقوة الاستراتيجية للفضاء السيبراني.

فقرة ثالثة: توقّعات المدنيين

هذا يشكّل تحدّيا آخر لسيادة الدولة في الفضاء السيبراني, انطلاقا من وجهات نظر عالمية, بشأن القدرة على الوصول الى الإنترنت بحريّة, وبدون كشف للهوية. فالقرارات الفرنسية, مثلا, بقطع اتصالات الإنترنت للأفراد الذين يستمرون في تحميل الأفلام والموسيقى بطريقة غير قانونية, أثارت صخبا في أوساط المعارضة.[٢٢٨] كما أنّ قانون الاتحاد الأوروبي, الذي يفرض على مزوّدي خدمات الانترنت, الاحتفاظ بمعلومات لمدة ١٢ شهرا, تتعلّق بالبريد الالكتروني, وزيارات المواقع, والإتصالات الهاتفية التي تجرى عبر الانترنت, أثار غضب المجموعات المتمسّكة بالخصوصية, مشبهة ذلك بنظام الغستابو.[٢٢٩] وإذا كان للدولة مصالح في فرض سيادتها على الفضاء السيبراني, فإنّ للأفراد أيضاً مصالح

[227] Franzese, Sovereignty in Cyberspace:Can it exist, p:37

[228] Pfanner,E. (Apr. 9, 2009) France Rejects Plan to Curb Internet Piracy, N.Y. TIMES.COM, http://www.nytimes.com/2009/04/10/technology/internet/10net.html?_r=0

[229] David Barrett, Internet Records to be Stored for a Year, TELEGRAPH, Apr. 5, 2009, http://www.telegraph.co.uk/technology/news/5105519/Internet-records-to-be-stored-for-a-year.html (last visited 16,10,2016)

تتعلّق بالخصوصية, التي يجب أن تؤخذ بعين الاعتبار, وأن تتم حمايتها وتأمين الضمانة لها, من خلال النظام الدولي.

فقرة رابعة: السيادة والمسائل التقنية ذات العلاقة

تواجه الدول تحدّيات تقنية متعددة أثناء محاولتها لفرض سيادتها على الفضاء السيبراني. ومن هذه التحدّيات:

- إنّ خلق نظام قادر ,على تحديد اللاعبين في الفضاء السيبراني بدقة, هو مهمّة شاقة.
- ترسم حدود الفضاء السيبراني, بشكل تستطيع الدولة مراقبته والتحكم به. فعدم التمكّن من القيام بهذه الوظيفة, يفرغ الفضاء السيبراني من مضمونه .[٢٣٠]

اذن, على الدول, أن تتجاوز عددا من المعوقات, لجعل السيادة في الفضاء السيبراني أمرا واقعا. فهناك حاجة الى نظام دولي, لبسط سيادة الدولةعلى هذا المجال. ورغم وجود عدد من القضايا التي لا بد من مواجهتها, في هذا المجال, يبقى العائق الأساسي, هو اعتقاد الدول أنّ السيادة في الفضاء السيبراني, والحوكمة الدولية لهذا الفضاء, تتعارضان مع مصالحها. كما يمكن للدول, أن تتخذ خطوات, لتطوير مفهوم السيادة السيبرانية . فأحاديا, يمكن للدولة أن تمارس السيطرة على حدود الفضاء السيبراني, من خلال خلق الوسائل, التي تمنع حركة مرور المعلومات, من مزودي خدمات ***الإنترنت Internet Service Providers (ISP),*** أو من الدول التي تنطلق منها الهجمات الالكترونية. كما يمكن للدول, أن تتوصل الى اجراء اتفاقات تعددية, للاعتراف بسيادة الدول في الفضاء السيبراني وذلك لمساعدة بعضها البعض, في تعقّب الهجمات السيبرانية من مصادرها الاساسية, من أجل تحديد اللاعبين المسؤولين عن هذه الهجمات بدقة, بغرض تسليمهم ومحاكمتهم. كما يمكن على الصعيد العالمي, أن تضع الأمم المتحدة مبادئ وقواعد, تشكل الركيزة التي تؤسّس لنظام دولي في الفضاء السيبراني.

[230] Franzese, Sovereignty in Cyberspace: Can it exist, p:40

المبحث الثاني: السايبر: الحرب القادمة

تشير التوقّعات الى أنّ الحرب السيبرانية, ستكون السمة الغالبة, إن لم تكن الرئيسة للحروب المستقبلية, نظراً للازدياد المطّرد للاعتماد العالمي على الفضاء السيبراني, لا سيّما في البنى التحتية المعلوماتية, العسكرية, والمصرفية, والحكومية, إضافة الى المؤسسات, والشركات العامة والخاصة. ولا شك أنّ ازدياد الهجمات الالكترونية, يرتبط بازدياد الاعتماد, على شبكات الكمبيوتر والانترنت, في البنية التحتية الوطنية الأساسية, وهو ما يعني إمكانية تطوّر الهجمات الالكترونية, اليوم, لتصبح سلاحاً حاسماً في النزاعات بين الدول, في المستقبل, علماً أنّ أبعاد مفهوم الحرب السيبرانية لا تزال غير مفهومة لدى شريحة واسعة من المراقبين, خاصةً مع الانقسام بين مؤيّدين ومشكّكين بوجود هذه الحرب.

المطلب الأول: حقيقةٌ أم تهويل

منذ عام ١٩٩٠, إدّعى أكاديميون, أن إقحام الفضاء السيبراني في الصراع, غيّر جذريا في كيفية خوض الحروب. فبالنسبة لـ***مالفانون وراتيري Mulvenon and Rattray***, غيّر الفضاء السيبراني, من السياسات والاقتصاديات والتفاعل الاجتماعي والأمن القومي, وأمّن فرصاً وامكانيات, وخلق تهديدات, وأوجد نقاط ضعف متعددة.[٢٣١]

وعام ١٩٩٣, أعلن كلّ من ***اركيلا ورونفلدت Arquilla and Ronfeldt***,[٢٣٢] أن الحرب السيبرانية قادمة. وهذه العبارة, أصبحت عبارة متداولة منذ نهاية الألفية الثانية, عند الحديث عن مقتضيات الأمن القومي. كما أن تزايد الاعتماد على تكنولوجيا المعلومات, لتأمين الخدمات الأساسية للمواطنين, أدّى الى تزايد الاهتمام بما سمي بالإرهاب السيبراني. وقد خشي رجال الأمن, من أن يؤخذوا رهائن على أيدي اللاعبين الحمر (نسبة للألوية الحمر) عبر الدخول غير المصرّح له الى بنى تحتية حيوية في البلاد, هذا أدّى الى تأسيس الجيش السيبراني, والميليشيات السيبرانية . حتى أن وزير الدفاع الأميركي, ***ليون بانيتا***

---

[231] Mulvenon, J. C., & Rattray, G. J. (Eds.). (2012). *Addressing Cyber Instability: Executive Summary*. Cyber Conflict Studies Association.

[232] Arquilla, J., & Ronfeldt, D. (1992). Cyberwar Is Coming', P-7795. *Santa Monica, CA: RAND*.

Leon Panetta , حذّر من حدوث "بيرل هاربور سيبرانية". [٢٣٣] أمر مبالغ به بالنسبة للبعض. ***فتوماس ريد Thomas Rid*** , يجادل أن الحرب السيبرانية, غير واقعية, لأن هذا الميدان غير قابل أن يحدث آثار عنف. " فالحرب السيبرانية لم تحدث في الماضي, وهي لا تحدث في الحاضر, ومن المستبعد أن تحدث في المستقبل". وجزء من هذا الادّعاء, مردّه الى الاعتقاد, أن الهجمات السيبرانية ليست عنيفة. [٢٣٤] كما يجادل ***اريك غارتزك Eric Gartzke*** , "أنّ الصراعات في الفضاء السيبراني, غير قادرة على ردع أو إرغام الخصم في العالم المادي", ولا تتناسب مع معايير ***كلاسويتز*** الثلاثة للحرب. ويمكن فقط فهمها كنماذج معقدة من التكتيكات التقليدية, كالتخريب والتجسّس. فبدلا من أن تغيّر في الحرب نفسها, تضيف بعدا آخر للقتال فيها.[٢٣٥]

حتى أنّ عددا كبيرا من الأكاديميين, يصرون أنّ ما يسمّى بالهجمات السيبرانية, ليست بالتهديد الكبير, فـ***بوزان وهانسن Buzan and Hansen*** , يؤيّدان هذا الرأي, ويعتبران أنّ الجدال القائم حول الهجمات السيبرانية, ينصب على إمكانات الإرهابيين من جهة, وضعف الأنظمة الرقمية الغربية, من جهة أخرى.[٢٣٦]

إن تعريف النواحي العديدة للحرب السيبرانية أمر اشكاليّ , وذلك لغياب اتفاقية دولية, تعنى مباشرة بالحرب السيبرانية. فحتى الآن, لم يتم التوصّل الى توافق حول أوجه الحرب السيبرانية. فقانون الحرب, والقانون الدولي التقليدي, يفتقدان لمبادئ مخصصة للحرب السيبرانية. وهناك خلاف حول ما اذا كانت كلمتا الهجوم السيبراني ***Cyber Attack*** , تشكّلان كلمة واحدة أم اثنتين. وما يمكن الكلام عنه, هو أن عبارتي ***jus ad bellum*** أي قانون الحرب ***وjus in bello*** أي قانون النزاعات المسلحة, تنطبقان على العمليات السيبرانية.

---

[233] Bumiller, E., & Shanker, T. (2012). Panetta warns of dire threat of cyberattack on US. *New York Times*, *11*, A1.http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0 (last visited 13,10,2016)

[234] Turner, M. (2014). Is There Such a Thing as a Violent Act in Cyberspace? *International Security and Intelligence Summer School 2013, Pembroke College, and the University of Cambridge*.

[235] Gartzke, E. (2013). The myth of cyberwar: bringing war in cyberspace back down to earth. *International Security*, *38*(2), 43

[236] Buijs,the relative power,p: 17

فليس هناك من تعريف متفق عليه عالميا للحرب السيبرانية, وإنما تعريف عام كالاتي :"الحرب السيبرانية هي اعتداء رقمي, منسّق, يشّن على حكومة ما, من قبل حكومة أخرى, أو من قبل مجموعة كبيرة من المواطنين. هي عمل تقوم به دولة لاختراق كمبيوترات وشبكات دولة أخرى, لإحداث ضرر أو اضطراب. وقد تستخدم عبارة الفضاء السيبراني, لوصف الهجمات التي تحدث ما بين الشركات, أو من قبل منظّمات ارهابية, أو ببساطة هي هجمات يقوم بها أفراد يدعون بالقراصنة, والذين تعتبر نواياهم حربية".[٢٣٧] وهناك من يعرّف الحرب السيبرانية, بالعمل المتماثل أو غير المتماثل, أدفاعياً كان أم هجومياً, والذي يتم من خلال الشبكة الرقمية, من قبل الدول أو اللاعبين من غير الدول, مشكلا خطرا على البنى التحتية الحساسة للدولة, وعلى أنظمتها العسكرية. وهذا الأمر يتطلّب درجة عالية من الاعتماد المتبادل, بين شبكات المدافع الرقمية وبناه التحتية, من جهة, كما تتطلب تقدما تكنولوجيا من الطرف المهاجم من جهة أخرى. "فالحرب السيبرانية هي تهديد مستقبلي أكثر منه حالي, ويصلح تسميتها أكثر بحرب المعلومات".[٢٣٨] أما وزارة الدفاع الأميركية, فتعرّف الحرب السيبرانية, بأنها "توظيف للإمكانيات السيبرانية, بهدف تحقيق أهداف عسكرية, من خلال الفضاء السيبراني".[٢٣٩] ويعرّف مجلس الأمن, في قرار صادر عنه الحرب السيبرانية بأنّها:" استخدام الكمبيوترات, أو الوسائل الرقمية, إمّا مباشرة من قبل الحكومة, أو على علم منها, أو بموافقتها, وذلك ضد دولة أخرى, أو مكان يقع ضمن سلطة هذه الدولة, ويتضمّن الدخول المتعمد, أو اعتراض البيانات, أو الإضرار بالبنى التحتية الأرقمية, او المتحكّم بها رقميا, كذلك هي انتاج وتوزيع الأجهزة, التي قد تستخدم لنشاطات تخريبية محلية."[٢٤٠]

كما يعرّف ***غاري سوليس Gary D. Solis***, الحرب السيبرانية بأنّها ليست الجريمة السيبرانية التي تعني استخدام الكمبيوترات, لخرق قواعد القانون المحلي, لأغراض إجرامية. ففي الولايات المتحدة

---

237 http://definitions.uslegal.com/c/cyber-warfare (last visited 17,10,2016)

238 Coughlan, S. M. (2016). *Is There a Common Understanding of What Constitutes Cyber Warfare?* Lulu Press, Inc. p:2

239 Joint Chiefs of Staff, Joint Publication 1-02, Dictionary of Military and Associated Terms (JP 3-0), Department of Defense, Washington D.C., 8 November 2010 p:58

240 UN Security Council, Resolution 1113 (2011), 5 March 2011

الاميركية, يعرّف قانون الاحتيال واساءة استخدام الكمبيوتر ,[241] الأفعال الجرمية على الانترنت. كما أنّ دول الاتحاد الأوروبي الأعضاء في حلف الناتو, لديهم قوانين محلية, تطبّق قانون حماية البيانات في الاتحاد الاوروبي ١٩٩٥.[242] وتتضمّن الجرائم السيبرانية النموذجية, تلك الجرائم المتعلقة بالبيانات, واساءة استخدام الاجهزة. أما الجرائم التقليدية, فهي الاحتيال, والمواد الاباحية, والتعدي على حقوق النشر, التي يسهلّها الدخول الى شبكة الانترنت.[243]

وعلى الصعيد العالمي, تعالج الاتفاقية حول الجرائم السيبرانية, الصادرة عن مجلس اوروبا لعام ٢٠٠١ الجريمة السيبرانية, وتكاد تكون الاتفاقية العالمية الوحيدة التي تعالج هذه المشكلة. ولكن يجب عدم الخلط بين مفهومي الحرب السيبرانية, والجريمة السيبرانية. فالحرب السيبرانية, يمكن تعريفها بأنها الحرب التي تشنّ في الفضاء, بما في ذلك الدفاع عن المعلومات وشبكات الكمبيوتر, وردع الهجمات المعلوماتية, فضلا عن إنكار قدرة الخصم على القيام بالأمر نفسه. ويمكن أن تشمل عمليات هجومية على معلومات العدو . اذا, تتضمّن الحرب السيبرانية الدفاع, والهجوم, والردع[244] وقد تشارك فيها دول, أو وكلاء دول, أو لاعبون من غير الدول, أو مجموعات. وهذا لا يعني أنها تشكّل إرهابا, ولكن قد تعني ذلك وفقا لتعريف الأرهاب. فوكالة إدارة الطوارئ الفدرالية الاميركية, تعرّف الإرهاب السيبراني, بأنه" الهجمات والتهديدات الغير قانونية, بحق الكمبيوترات والشبكات والمعلومات المختزنة فيها, والتي تجري من أجل إثارة الرعب أو الإكراه, بحق الحكومة أو شعبها لأهداف سياسية أو اجتماعية".[245]

---

241 Smit, H. (1965). International Litigation Under the United States Code. *Columbia Law Review*, *65*(6), 1015-1046. https://www.law.cornell.edu/uscode/text/18/1030 (last visited 13,10,2016)

242 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

243 Jonathan, C. (2010). Principles of Cybercrime.

244 Solis, G. D. (2014). Cyber warfare. *Mil. L. Rev.*, *219*, 1.p: *3-4*

245 Wilson, C. (2008, January). Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE. https://www.fas.org/sgp/crs/terror/RL32114.pdf (last visited 13,10,2016)

أما ***رتشارد كلارك Richard Clarke*** , فيجادل بأن "الحرب السيبرانية, هي نوع جديد من القتال لم نفهم بعد الآثار المترتبة عليه".[٢٤٦] لكن الحرب السيبرانية, لا تختلف كثيرا عن اشكال الحرب التقليدية. فالفضاء السيبراني وسّع مجال المعركة فقط, ويجب أن ينظر اليها كساحة حرب خامسة, بموازاة المجالات التقليدية البرية والبحرية والجوية والفضائيّة. فالحرب السيبرانية, اذا, جديدة, ولكن ليست مكونا منفصلا كليا عن بيئة الصراع المتعددة الوجوه.

وقد عرّف كتيّب ***تالين***, الحرب السيبرانية على أنّها : " كلّ العمليات السيبرانية سواءا كانت دفاعية أو هجومية والتى يعتقد أنّها قد تسبّب اصابات أو وفيات للبشر أو تلف وضرر للأشياء المادية". هذا التعريف غير كاف, للإحاطة بأشكال الاشتباك والصراع الدائرة حاليا, فهو يغفل العنصر الأهم فى أمن المعلومات, وهو العامل البشرى النفسى. وأزمة التعريف, تنبع من أهمية التمييز بين أشكال الحرب السيبرانية و أشكال اخرى, مثل الحروب النفسية, وحروب المعلومات, وايضا أشكال الجريمة السيبرانية, والإرهاب السيبراني, والحدود الفاصلة بينها, ومتى تتوقّف حدود إحدى هذه الأفرع, و تبدأ حدود فرع آخر, لتحديد إمكانيات واشكال التنسيق, و مهام عناصر القيادة, وعمليات التحكّم بمختلف القطاعات العسكرية, وحتى الاقتصادية والمدنية منها.

اذاً, مع غياب التعريف الموحّد, تبدو هذه الحرب, عمليا, كامتداد لحرب الاستخبارات, وكميدان جديد للنزاعات, يأخذ مكان الحرب الباردة. أمّا مميزاتها, "فهي أنّها سريّة, وخفيّة, ومحاطة بالكثير من المغالطات والتضخيم".[٢٤٧]

ففي الحقيقة, إنّ معظم الاعتداءات السيبرانية, لا تحدث أضرارا مادية يمكن لمسها. فطبيعة الفضاء السيبراني, والمصالح المتصلة به, شديدة التعقيد, نظرا لامتدادات البنية التحتية, وتشابكها, ونظرا للتقنية العالية, وسرعة تطورها, وامكانات تمويه مصادر الاعتداءات. هذا عدا عن صعوبة تحديد ما الذي يمكن اعتباره عملا عسكريا, أو اعتداء, أو حربا سيبرانية. فالسرقات التي تطال المصارف, وعمليات التجسّس الصناعي, ليست أعمالا حربية, بالرغم من أبعادها الخطيرة على الأمن القومي, لأنّها تمس الاقتصاد الوطني, ورفاه البلد, إلاّ أنّ الخبراء يرون انعكاسات الاعتداء على البنك المركزي الاميركي, مثلا, أشد وأدهى من اعتداءات الحادي عشر من سبتمبر, على الاقتصاد العالمي. فالهجمات على استونيا,

---

[246] Clarke, War from cyberspace,P:32

[247] د. الأشقر جبور منى, السيبرانية هاجس العصر, المركز العربي للبحوث القانونية والقضائية, ص:٦٦-٦٧

وجورجيا, وايران, لم تتسبّب بأضرار بشرية, ولم تذكر لها نتائج خطيرة على المدنيين, ولكن يمكننا تصوّر نتائجها الوخيمة على السلام, لو اعتبرت هذه الاعتداءات حربا, كونها استهدفت تعطيل مواقع ,ومصالح حيوية, ومنها تلك الخاصة بالقوات المسلحة, او فيما لو اعتبرت الهجمات, من فعل جيش سيبراني معيّن, استخداما للقوّة.[٢٤٨]

فالدول التي تعد وحدات سيبرانية أو خبراء إنترنت ماهرين للقتال في هذا الميدان, هي في تزايد مطّرد."[٢٤٩] فإعلان الولايات المتحدة الاميركية, أنها تستخدم الوحدة السيبرانية العسكرية التي أنشأتها عام ٢٠٠٩, والتي تعرف ***بالسيبركوم Cybercom*** , والتي تتّبع الوحدة الاستراتيجية الامريكية ضمن وزارة الدفاع الاميركية, لشن هجمات الكترونية ضد الدولة الاسلامية, هو دليل على أهمية هذه المعركة الجديدة. فرغم استمرار الولايات المتحدة الاميركية, في استخدام الاسلحة التقليدية ضد الدولة الاسلامية, إلاّ أنّها تطمح الى استهداف أنظمة المنظمة المعلوماتية, الموظفة عسكريا وماديا, والحاق أضرار جسيمة بها. فالولايات المتحدة, هي واحدة من الدول التي تستثمر أموالا طائلة, في تطوير, ليس فقط القدرات الدفاعية في وجه الهجمات السيبرانية, بل ايضا تطوير القدرات الهجومية كذلك.

اذاً من الأهمية بمكان, أن نميّز, بين الحرب السيبرانية والحرب غير السيبرانية, في الفضاء السيبراني. فمثلا, يمكن للأفعال السيبرانية التي تقوم بها المجموعات الإرهابية, والجواسيس والمجموعات الإجرامية, أن تكون مؤذية, وقد تبدو عدائية, ولكن ليس من الضروري أن تشكّل وحدها عملا حربيا في الفضاء السيبراني. فالحرب السيبرانية, هي نموذج للحرب الغير متماثلة, حيث الخصم ضعيف, لكن في نفس الوقت على درجة عالية من الذكاء والخفّة, بينما الطرف الأخر قوي , لكن غير مرن وراض عن نفسه. فما يميّز الحرب السيبرانية, هو السرعة التي يمكن أن تتطوّر فيها التهديدات. وهناك جدل قائم وخطير وخادع, حول أنّ هذا النوع من الحروب, يفضّل اعتباره كشكل من أشكال الصراع غير الدموية, والتي لا تؤلم, ولكن تقدم نتائج حاسمة, حيث الإعتراف بالنصر أو بالهزيمة, بعيد كل البعد عن الفضاء السيبراني. وهذه المفاهيم, لا تنسحب على ميدان حيث المحاربون السياسيون والفكريون والدينيون والاقتصاديون والعسكريون يتقاتلون, لأسباب عديدة, ووفقا لفترات زمنية مختلفة, مطبّقين قواعد من القتال خاصة بهم.

---

[248] Schreier, *On cyberwarfare*.p:16,17

[249] Lewis, J. A., & Timlin, K. (2011). *Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organization*. UNIDIR.

المطلب الثاني: حرب غير تقليدية

يستخلص التقرير الصادر عن مركز ***شاتم*** ,الخصائص التالية للحرب السيبرانية:

- الحرب السيبرانية تمكّن اللاعبين من الوصول الى أهدافهم السياسية والاستراتيجية, بدون الحاجة الى الإنخراط في صراع مسلّح.
- الفضاء السيبراني يعطي قوة غير متماثلة, للاعبين صغار وغير مهمّين.
- الغموض الذي يحيط باللاعبين بسبب التخفّي وراء عناوين IP , وأسماء مستعارة, وخوادم أجنبية.
- عدم وضوح الحدود الفاصلة بين ما هو عسكري, وبين ما هو مدنيّ وبين ما هو ماديّ, وما هو افتراضيّ, والقوّة الممارسة من قبل الدول, أو تلك الممارسة من قبل اللاعبين من غير الدول, أو عبر الحرب بالوكالة.
- الحرب السيبرانية تفهم كميدان جديد للحرب, ولكن بمكوّنات غير مستقلة تماما عن بيئات الصراع التقليدية, من بر وبحر وجو وفضاء.
- إنّ الأعمال الشبيهة بالحرب في الفضاء السيبراني يمكن ان تحصل بالتزامن مع اشكال أخرى من المواجهة والإكراه.[٢٥٠]

ويضيف ***سكراير*** , الى ما ورد, خصائص اخرى:

- الحرب السيبرانية قليلة التكلفة, فلا تتطلب عددا كبيرا من القوات والأسلحة. كما أن الدخول في الحرب أمر غير مكلف, فبوجود كمبيوتر, واتصال بشبكةالانترنت, يمكن لأي كان, ومن أي مكان في العالم, أن ينخرط في حرب سيبرانية.
- تمكّن الحرب السيبرانية اللاعبين, من تحقيق أهداف سياسية واستراتيجية, من دون الحاجة الى الانخراط, في نزاع مسلح.
- الحرب السيبرانية لا تحتاج الى ساحة للمعركة. فالأنظمة التي تدخل في صميم حياة الناس من مصارف الى محطات توليد الكهرباء, الى رادارات الدفاع الجوي, يمكن الدخول اليها عبر الفضاء

[250] Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010). *On Cyber Warfare* (pp. 21–22). Chatham House. p:9

السيبراني وبالتالي يمكن استحواذها او تدميرها, دون الحاجة لإلحاق الهزيمة, بدفاعات الدولة التقليدية.[٢٥١]

ولقد أسفر الفضاء السيبراني عن تغيير في مضمون القوات النظامية, أي الجيوش بمختلف أشكالها وتشكيلاتها, والقوات المتطوّعة, التي تتكوّن من أفراد يعملون بدافع وطنيتهم مع الجيوش النظامية. فصحيح أن الفرق الجوهري بين القوات العسكرية التقليدية ومشغّلي برامج المعلوماتية, لم يتغيّر من حيث الأغراض والأهداف, إلاّ أنّ البنية والروابط مع الدولة, قد تغيّرت جذريا في عصر الفضاء السيبراني. ففي الماضي كان نقص عديد القوات العسكرية يحدث خللا أمنيا, ويهدّد أمن الدولة بالتفكّك, أمّا اليوم فلم يعد للعديد أي قيمة استراتيجية تذكر, لأن الفضاء السيبراني قلّل من مفعول الترابط بين قدرة الجيش وعديده وعزّز قدرة الدولة الواحدة, المالكة لهذا السلاح الحديث, أو القابضة عليه, على ضمان أمنها والدفاع عن نفسها بمفردها. وصار بإمكان دولة صغيرة مستضعفة, أن تواجه منفردة دولة متفوّقة عسكريا, بعد قيامها بإنتاج برامج معلوماتية متعددة الغايات والأغراض وستحرر, اذا, تكنولوجيا الفضاء السيبراني الدول الصغيرة, حسنة التنظيم والتدبير نسبيا, من الاعتماد على حلفائها الإقليميين.[٢٥٢]

ولنفهم ما اذا كان الفعل العدائي في الفضاء السيبراني, فعلاً حربياً, لا تكفي مراقبة الحدث فقط, بل لا بد من فهم نيّة اللاعب. فالحرب السيبرانية من الوجهة ***الكلوسويتزاينية Clausewitzian***, هي "فعل قوة لفرض اراداتنا على العدو". فيجب أن نؤكد نيّة اللاعب, أو إرادته في الصراع, قبل القول إنّ ما يجري هو عمل حربي, أو غير ذلك. فاذا كانت نيّة المهاجم السيبراني, هي الحصول على منفعة شخصية أو مادية, من خلال وسائل إجرامية: كالسرقة والاحتيال والابتزاز, فالنيّة يجب أن تكون واضحة بشكل كاف, والهجوم يجب أن يرى على أنه عمل اجراميّ, والتعامل معه يكون على هذا الأساس. ولكن, اذا كان لدى المهاجم طموحات اكبر, ويصبو الى إحداث اذىً كبيراً للدولة, أو مواطنيها, أو تعطيل أو تقويض هياكل وبنى تحتية مدنية, أو عسكرية, يصبح من المناسب وصف هكذا تصرف, بأنه أمر يقرب من العمل الحربي بالمعنى التقليدي. فيجب التمييز بين الأفعال التي تبدو أنها مرتكبة بدافع عدائي, وتكون أحداثا

---

[251] Schreier, On Cyberwarfare,p:28

[252] المجذوب, السايبر ساحة خفية لحرب ناعمة قادمة!

معزولة, وبين تلك التي تشكّل حرباً حقيقية, والتي تتطلّب اعترافا متبادلا, لا يلتبسه الغموض, من قبل المعتدي والمدافع, بوقوع حرب.[٢٥٣]

وتكمن جاذبية الفضاء السيبراني, في عنصر الغموض الذي يقدمه, على الأقل على المدى القصير. ففي حالة الشك في رعاية إحدى الدول للهجمات السيبرانية, من الصعب التأكيد أنّ أمر الهجوم صدر عن المكتب الرئاسي, أو التنفيذي لدولة ما. كذلك فإن صعوبة الإسناد, تسمح للدولة المشكك بها أن تنكر تورطها بذلك. فيمكن للجناة إخفاء أي أثر لهم, بل وتوريط اخرين بذلك, خاصة إذا ما استخدمت كمصدر للهجمات, خوادم وبوتنت ,تابعة لطرف ثالث, و تقع في دول لا علاقة لها بالعمل.

ويعتقد أن الولايات المتحدة,الصين, روسيا, اسرائيل, والمملكة المتحدة, هي الأكثر تقدما في امتلاك إمكانات الحرب السيبرانية, مع أهمية كلّ من ايران وكوريا الشمالية كذلك.هذه القوى السيبرانيّة, تجاوبت مع عدد متزايد من الهجمات, في السنوات الماضية.

إنّ ممارسات الدول اليوم, تظهر أنها تتردّد في تحمّل المسؤولية عن الأعمال السيبرانية, التي تأتي من داخل أراضيها. ففي الإعتداء السيبراني على استونيا, لم تتحمّل روسيا أية مسؤولية, حتى أنها لم تتجاوب مع مطالبة استونيا لها, للتحقّق من المعتدين, الذين قاموا بالعمل من داخل أراضيها. كذلك فأنّ العديد من خبراء الانترنت, كانوا قد نسبوا هجوم ***ستكسنت*** على المنشأة النووية الايرانية , الى كلّ من الولايات المتحدة الأميركية وإسرائيل, الاّ أنّ أي من البلدين, لم يقرّ بمسؤوليته عن هذا العمل.[٢٥٤] فموضوع إسناد العمل السيبراني فيه الكثير من الصعوبة, خاصة أنّ طبيعة الإنترنت تحمل الكثير من الغموض, هذه الخاصية التي تعتبر دعوة مفتوحة, لكلّ من يرغب في التسبب بضرر, مهما كانت دوافعه. إنّ صعوبة الإسناد, تجعل الدول حذرة في تقبّل مسؤولية الهجوم السيبراني, من داخل أراضيها, لضعف قدرتها على تحديد المهاجم, في الوقت المناسب. فحتى لو تمكّنت الدولة من تحديد الكمبيوتر الذي نشأ عنه فعل الهجوم , فإنها من غير المرجح, أن تعرف من يقف وراء جهاز الكمبيوتر.[٢٥٥] كذلك إنّ الغموض هذا,

---

[253] المصدر نفسه,ص:١٣

[254] Nakashima, E., & Warrick, J. (2012). Stuxnet was work of US and Israeli experts, officials say. *Washington Post*, *2*. http://www.washingtonpost.com/world/national-security/stuxnet-was-work-ofus-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

[255] Jensen, E. T. (2012). Cyber Deterrence.REV. 773, 785-86 (2012)

يسمح للدول أن تقوم هي بالعمل, مدركة صعوبة التحديد الزمني. هذا ينطبق خاصة, على الدول التي تقوم بالعمل بالوكالة من خلال اللاعبين من غير الدول. كما أنّ طبيعة تدفّق المعلومات على شبكة الإنترنت, تجعل الدول متردّدة في تقبّل المسؤولية, عن النشاطات السيبرانية التي تتدفّق من أراضيها. فإرسال بريد إلكتروني من كمبيوتر في مدينة معينة, الى متلقّ في المدينة نفسها, يمكنه أن يقطع عددا من الدول الاجنبية قبل وصوله الى وجهته المقصودة. الأمر نفسه ينطبق على الجرائثيم الخبيثة السيبرانية, التي تصعب السيطرة عليها من قبل مرسلها لجهة كيفية سفرها, ومن قبل الدول التي تمر عبرها ايضا. هذا يعني, أنّ هذه الجرائثيم يمكنها أن تقطع عدة دول, قبل الوصول الى الدولة المستهدفة. فدول العبور لا تريد ان تكون مسؤولة عن هذه البيانات الضارة, في سيناريو كهذا.[٢٥٦]

المطلب الثالث: ساحةٌ صراعٍ جديدة

إنّ مجيء الحرب السيبرانية, أدّى الى ظهور الفضاء السيبراني كميدان جديد للقتال, بميزات جديدة, جعلته ميدان قتال فريد من نوعه, وذلك للأسباب الآتية:

- الفضاء السيبراني هو في كلّ مكان, ومفتوح لأي كان, سامحا لمستخدمين أن يتحركوا عبره بسهولة, وبسرعة هائلة. ولأنه ميدان مفتوح للجميع, يمكن للدخلاء الوصول الى أنظمة وشبكات حساسة, حيث يصعب كشفهم, أو حتى طردهم منه.
- الفضاء السيبراني يؤمّن معركة واسعة, بدون حدود, تشكّل ملاذا آمنا, فلا بد للمدافعين أن يبنوا جدرانا نارية, علما أنه يمكن اختراقها, أو تجاوزها.
- إنّ تكنولوجيا المعلومات, هدمت الوقت والمسافة في الحرب السيبرانية. ففي هذا الميدان الجديد من العمليات, قلّلت سرعة الانترنت, من أهمية المسافات. فالاقتحامات تأتي بوتيرة عالية, وسرعة كبيرة, حتى أن قوى الدفاع السيبرانية, لا تمتلك إلاّ ثوان قليلة للرد.
- التغيير المتعدّد الأشكال لمكوّنات الفضاء السيبراني , والتي هي في تحوّل مستمر. فهذه المكونات, يتم خلقها, وتحديثها, وتحريكها, وتغيير موقعها, وتدميرها, وقطعها, واعادة وصلها, وتخبئتها, وكشفها باستمرار, نتيجة للتجدّد المستمر في تكنولوجيا المعلومات, والتي تنعكس بدورها

---

[256] Jensen, Cyber Sovereignty: The Way Ahead,P:278

على تطوّر الفضاء السيبراني. هذا التعدّد يجعل التهديدات, ومكامن الضعف في الفضاء السيبرانيّ, تختلف عن عالم القتال التقليدي. فاذا ما قارنا ميدان الفضاء السيبراني الحربي, بميادين الحروب الأخرى , نجد ان الفضاء السيبراني, يؤلف بيئة يصعب فيها تحقيق الأمن, ويصعب الدفاع عنها , حيث يصعب الدفاع عن مكان لا حدود له, يتواجد افتراضيا في كلّ مكان, ويسمح لأيّ كان بدخوله. وحتّى ما يسمّى بالشبكات المغلقة, هي ايضا معرضة للخطر, من خلال إدخال الجراثيم الخبيثة اليها عبر أجهزة تخزين محمولة, أو عبر شيفرة تنتقل من خلال تردّدات الرادار أو الراديو.[٢٥٧]

المطلب الرابع: أنماط الصراع السيبراني

يصنّف ***عبد الصادق***, أنماط الصراع في الفضاء السيبراني, من حيث تعرّضه لأنماط الحرب والصراع, الى ثلاثة:

فقرة أولى: صراع منخفض الشدة

حيث يتم استخدام الفضاء السيبراني كساحة للصراع الغير السلمي. ويتميّز هذا النمط بدرجة من التعقيد, ولا يتطوّر بالضرورة الى حالة استخدام القوة المسلّحة, بشكلها التقليدي, أو الى شن حرب سيبرانية واسعة النطاق. هذا النمط قد يأخذ شكل حرب اعلامية ونفسية, أو قد يصل الى حد الاختراق من أجل سرقة أسرار صناعية, أو قد يأخذ طابعاً تنافسياً عالميّاً بين الشركات التكنولوجية, عبر الفضاء السيبراني. كذلك قد يصل الصراع على المعلومات والنفوذ الى أجهزة الاستخبارات الدولية. وقد يترجم العداء المتبادل بين الدول, الناجم عن صراع سياسي ذي بعد اجتماعي – ديني, كالصراع العربي الاسرائيلي, أو الصراع بين الهند وباكستان, أو بين كوريا الجنوبية والشمالية, في شكل اختراقات الكترونية, أو عبر توظيف القراصنة, في شنّ هجمات بهدف السرقة, وتحقيق مكاسب مالية, الى جانب امكانية توظيفهم لصالح جماعات, أو أجهزة أمنية تابعة لدول بعينها. كما قد يأتي هذا النمط, في إطار محاولة الدول المتقدمة, اختبار دفاعاتها ضد الهجمات, التي يستخدم فيها الكمبيوتر سلاحا دفاعيا , عبر شن هجوم على الأقمار

[257] Schreier, *On cyberwarfare*. P:95

الصناعية الخاصة بالاتصالات, أو محطات البثّ, أو كابلات الاتصالات.[٢٥٨] خاصة أنّ تحقيق السيطرة على الشبكات, يمكّن من السيطرة على الأسرار العسكرية والعلمية, بما يقود الى أن تصبح الحرب المستقبلية باهظة التكاليف.[٢٥٩]

ب- صراع متوسّط الشدّة

حيث يتحوّل الصراع عبر الفضاء السيبراني الى ساحة موازية لحرب تقليدية دائرة, تعبيرا عن حدّة الصراع القائم بين ألاطراف, وقد يكون مقدّمة لعمل عسكري. وتدور حرب عبر الفضاء السيبراني, عن طريق اختراق المواقع, وقصفها, وشنّ حرب نفسية, وغيرها. ويستمد ذلك الصراع سخونته من قوة أطرافه وارتباطه بعمل عسكري. فيمكن للدول تمويل حملة حربية كاملة عبر الإنترنت, بتكلفة دبابة واحدة, وبوقت أقلّ. وتاريخيا, تم استخدام هذا النمط من الهجمات من قبل حلف الناتو, عام ١٩٩٩ على يوغوسلافيا, حيث استهدفت الهجمات شبكات الاتصالات, وعطلتها, ما أدى تلقائيا لتوقف شبكات الجيش.[٢٦٠] كما استخدم في الحرب بين حزب الله واسرائيل عام ٢٠٠٦ , وفي الهجمات السيبرانية الروسية على استونيا وجورجيا, وبين حماس واسرائيل عام ٢٠٠٩, و في الحرب بين غزة وإسرائيل, عام ٢٠١٢. كذلك في الصراع ما بين المعارضة السورية والنظام السوري, عبر استخدام الفضاء السيبراني, من قبل العديد من التيارات, للحشد والتعبئة, وكمنصة للصراع فيما بينها.[٢٦١]

ج- صراع مرتفع الشدة

يتميّز هذا النمط من الصراع, بسيطرة البعد التكنولوجي على إدارة العمليات الحربية, حيث يتم استخدام الأسلحة الالكترونية, فقط, ضد منشآت العدو, ويتم استخدام الروبوتات الآلية في الحروب, والتي يتم

---

[258] عبد الصادق,الفضاء الالكتروني والعلاقات الدولية,ص: ٢٤١-٢٤٢

[259] Greenberg, A. (2012). Forbes. Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits. http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#3a29ac706033 (last visited September 1,2016)

[260] Bieber, F. (2000). Cyberwar or sideshow? The Internet and the Balkan wars. *Current History*, *99*, 124.

[261] عبد الصادق,الفضاء الالكتروني والعلاقات الدولية, ص:٢٤٣

إدارتها عن بعد, فضلا عن الطائرات بدون طيار, ويتم تطوير القدرات في مجال الدفاع, والهجوم الالكتروني, والاستحواذ على القوّة الالكترونية. ويتم استخدام الفضاء السيبراني, في الاستعداد لحرب المستقبل, والقيام بتدريبات على توجيه ضربة أولى لحواسيب العدو, واختراق العمليات العسكرية, العالية التقنية, أو حتى باستهداف الحياة المدنية, والبنية التحتية المعلوماتية. ولعل الهدف من وراء ذلك تحقيق الهيمنة الالكترونية الواسعة, بشكل أسرع, في حالة نشوب صراع. ويشكل هجوم ستكسنت stuxnet نموذجا لهذا النمط من الصراع.[٢٦٢]

262 عبد الصادق,الفضاء الالكتروني والعلاقات الدولية,ص:٢٤٤

المبحث الثالث: السلاح السيبراني

إنّ الكلام عن الحرب السيبرانية, يفترض حكماً التطرّق الى السلاح المستعمل, القادر على إحداث خسائر فادحة. فعلى الرغم من بساطة هذا السلاح, فهو لا يتعدّى في أغلب الأحوال "الكيلو بايتس", الذي يتمثّل في فيروسات إلكترونية, تخترق شبكة الكمبيوتر، وتنتشر بسرعة بين الأجهزة، وتبدأ عملها في سرية تامة وبكفاءة عالية، وهي في ذلك لا تفرق بين المقاتل والمدني، وبين العام والخاص، وبين السري والمعلوم. ومن هنا, أتطرّق في هذا المبحث, الى ماهية السلاح السيبراني وميزاته, والأهداف المتوخاة من استخدام الدول والمنظمات والأفراد له, وأطرح تساؤلات حول فوائد استخدامه وسعة تأثيره. مع الإشارة الى أنّ التطوّر التكنولوجي المستمرّ, يستتبع تحديثاً للأسلحة الموجودة, وخلقاً لأسلحة جديدة, لا سيّما في كلّ مرّة يتم فيها ايجاد نظام دفاعٍ أو حماية في وجه السلاح المستخدم.

المطلب الأول: ماهيته

يعرّف كتيّب ***تالين Tallinn*** , الأسلحة السيبرانية بأنها "وسائل سيبرانية, لحرب مصمّمة, ومستخدمة, بنيّة التسبب بجرح أو موت الناس, أو تدمير, أو الحاق الضرر بالاشياء".[٢٦٣] اذن, نحن في صدد اختبار سلاح سيبراني, اذا تم إحداث اصابات, أو تعطيل وظائف كمبيوتر, من خلال هجوم سيبراني متعمّد. ولكن كما ذكرنا سابقا, فإنّ عنصري الإسناد والنيّة قد يكونان مجهولين, إضافة الى أن الهجمات السيبرانية, غالبا ما تخلق آثارا, لم يكن للمهاجم نيّة في إحداثها. فتحليل الشيفرات الخبيثة للهجمات السيبرانية المعقّدة, التي حدثت في السنوات الماضية, كشفت عن أربعة عناصر, تساعد في إعطاء تعريف أوضح, للسلاح السيبراني. فاذا ما اجتمعت هذه الخصائص, عندها يمكن اعتبار ما تم استخدامه في الهجوم سلاحا سيبرانيا:

- القيام بعملية سيبرانية, عبر برامج خبيثة, بغرض التجسس, أو سرقة البيانات, أو التخريب.
- امكانية التسلّل والتخفّي, لتشغيل برامج خبيثة تم زرعها داخل منظومة معينة .
- أن يملك المهاجم معرفة وثيقة, بتفاصيل عمل المنظومة المستهدفة.

---

[263] Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press. P:142

➢ وجود نوع خاص من رموز الكمبيوتر, لتجاوز تكنولوجيا الأمن السيبراني الوقائي.[٢٦٤]

و لعل التعريف الأكثر قبولا للسلاح السيبراني, هو التعريف الذي أورده كلّ من ***توماس ريد وبيتر ماكبرني*** ***Thomas Rid and Peter McBurney*** , بأنه:" شيفرة كمبيوتر, تستخدم, أو مصمّمة للاستخدام بهدف التهديد, أوالتسبّب بأذى مادي أو وظيفي أو عقلي للهياكل, والأنظمة, والكائنات الحية".[٢٦٥] ومن الأمثلة عن هذه الأسلحة , هجمات تعطيل الخدمة, وإدخال الجراثيم الخبيثة, المصمّمة لتدمير أنظمة المعلومات, أو المعلومات المخزّنة فيها.

المطلب الثاني: أنواعه

يصنّف ***ريد وماكبرني,*** الأسلحة السيبرانية, في قائمة طويلة, حيث نجد في أدناها, البرمجيات الخبيثة, التي تستطيع التأثير في النظام من الخارج, دون التمكن من اختراقه, والتسبب بضرر مباشر لها. فالبرنامج يستخدم لإثقال الخادم, دون أن يلحق ضرراً مادياً أو وظيفياً, بكائن حي, أو هيكل أو نظام. إنّه إبطاء مؤقت لنظام, أو إغلاق له, دون الإضرار به مباشرة, كهجوم تعطيل الخدمة, الذي قد يستهدف موقعاً مصرفياً, مثلا, لتشويهه و الإضرار بسمعته, اضافة الى التجسّس, أو سرقة ملكية فكرية. وقد يكون اعتداء ***استونيا*** عام ٢٠٠٧, مثالا على ذلك.

أمّا في أقصاها, فنجد البرامج الخبيثة, القادرة على خرق الأنظمة الأكثر حماية, والأكثر عزلة, وإلحاق ضرر مباشر بها. ومن الأمثلة, تسبّب جهاز الاستخبارات الأميركي بتفجير خط الأنابيب السوفياتي, ***ترانس سيبارين*** ,عام ١٩٨٢, والذي تم, من خلال الضغط الهائل المتعمّد للانابيب, عبر التلاعب بصمامات التحكّم بالضغط. ومثال آخر, هو الهجوم السيبراني الإسرائيلي, على جهاز الدفاع الجوي السوري عام ٢٠٠٧, الذي استهدف التعطيل المؤقّت, لمحطّة الرادارالتابعة لجهاز الدفاع الجوي. والمثال الثالث والأشهر, هو هجوم ستكسنت, الذي استهدف أجهزة الطرد النووية الايرانية .

---

264 https://gcn.com/Articles/2015/06/04/Cyber-weapon.aspx?Page=1

265 Rid, T., & McBurney, P. (2012). Cyber-weapons. *the RUSI Journal*, *157*(1), 6-13. https://www.rusi.org/downloads/assets/201202_Rid_and_ McBurney.pdf

وما بين أدنى القائمة وأقصاها, نجد الاختراقات العالية التكلفة, كالاختراق الذي جاء على يد طالب فيليبيني من مانيلا,حيث انتشرت في٤ ايار ٢٠٠٠, دودة I love u ,عالميا, لتصل في يوم واحد الى ٤٥ مليون كمبيوتر, وذلك من خلال ارسال الرسائل الالكترونية على شكل رسالة حب من مجهول, الى كلّ من ورد اسمه, في دفتر عناوين صاحب الكمبيوتر. هذا الهجوم, تسبّب باضرار مادية عالمية, تخطت العشرة بليون دولار. وألحق الفيروس, ضرراً بأنظمة كمبيوتر في البنتاغون, وجهاز الإستخبارات الأميركي.[٢٦٦]

كما يرى كل من ***ريد وماكبرني*** ضرورة التمييز بين ما يوصف بأنه سلاح سيبراني وما هو غير ذلك. وبرأيهما أن التمييز هام للأسباب التالية:

- أمنيا, فالوسيلة المستخدمة تصبح أقل خطرا , عند عدم استخدامها كسلاح قد يتسبب بإلحاق الأذية بأحد .
- سياسيا, فالاختراق غير المسلّح هو سياسياً, أقل خطرا.
- قانونيا, فتحديد شيئ ما بأنه سلاح, يجعل حيازته, أو استخدامه, أو تصنيعه خروجا عن القانون, ويعرّض صاحبه للعقاب.

فحتى أكثر الجراثيم الخبيثة تعقيدا لا تعتبر سلاحا. ومن الأمثلة : ***Duqu*** , الذي اكتشف عام ٢٠١١ في هنغاريا , وهو عبارة عن جرثومة خبيثة, تقوم بجمع معلومات استخبارية من مصنعي أنظمة التحكم الصناعية. و ***Bundestrojaner*** ,وهو برنامج بامكانه تسجيل المكالمات الصوتية عبر الانترنت, والذي اتهمت الشرطة الالمانية باستخدامه, للتجسّس محليا على المكالمات الصوتية لمشتبه بهم, وقد اعترفت بالقيام به فيما بعد. هذان البرنامجان لا يعتبران سلاحا, بسبب عدم نيّة استخدامهما لخلق ضرر مادي, وقد استهدفا,فقط, جمع معلومات بطريقة معقدة.[٢٦٧]

---

[266] Ibid,p:6

[267] Ibid,p:7

وتشمل الأسلحة السيبرانية, برامج تمّ تصميمها للقيام بوظائف مختلفة, ومنها, على سبيل المثال لا الحصر:

أ- فيروسات الحاسوب ***viruses***

هي برنامج ينتشر من كمبيوتر الى آخر متدخلا بعمله, حيث يمكن له أن يفسد, أو يمحو البيانات الموجودة عليه, كما يمكنه من استخدام برنامج رسائل البريد الالكتروني, لينشر الفيروس الى كمبيوترات أخرى, أو حتى أن يمحو كل البيانات الموجودة, على القرص الصلب. وغالبا ما تنتشر هذه الفيروسات, من خلال مرفقات رسائل البريد الالكتروني, متنكرة بصور مضحكة, أو بطاقات ترحيب, أو ملفّات صوت وأفلام. وقد تنتشر ايضا من خلال عملية التحميل عن شبكة الإنترنت, مختبأة في برنامج قرصنة, أو في الملفات, أو البرامج يتم تحميلها .[٢٦٨]

ب- الديدان ***worms***

هي برامج خبيثة صغيرة لا تعتمد على غيرها وتتكاثر بنسخ نفسها عن طريق شبكات الكمبيوتر, وقد صنعت للقيام بأعمال تخريبية, كأن تعمل على قطع الاتصال بالشبكة, أو سرقة بعض البيانات الخاصة بالمستخدمين, أثناء تصفحهم للانترنت. وتمتاز بسرعة الانتشار, وبصعوبة التخلّص منها, نظرا لقدراتها على التناسخ والمراوغة. غالبا ما تستهدف الشبكات المالية التي تعتمد على الكمبيوتر, مثل شبكات البنوك. ومن أشهرها دودة موريس ***Morris*** عام ١٩٨٨, ودودة نيمدا ***Nimda*** عام ٢٠٠١, ودودة ستكسنت ***Stuxnet***.[٢٦٩]

ج- أحصنة طروادة ***Trojan horses***

هي شيفرة, أو برنامج صغير متنكّر ببرنامج شرعي, يستخدمه اللصوص السيبرانيون والقراصنة, في التمكن من الوصول الى أنظمة المستخدمين. فعندما يتم تنشيطه في الكمبيوتر, يمكن للمجرمين

---

268 What do computer Virsus do and how to remove and avoid computer viruses? http://miamicomputerrepairsite.com/what-do-computer-viruses-do-how-to-remove-and-avoid-computer-viruses/comment-page-18/ (last visited September 4,2016)

269 **What Are Computer Worms, and How Do They Work?** **https://www.lifewire.com/how-computer-worms-work-816582**

السيبرانيين, التجسّس على المستخدم, وسرقة بياناته, أو محوها, أو حجبها, أو تغييرها, أو نسخها, أو الاخلال بآداء الكمبيوتر, أو شبكة الكمبيوتر.[٢٧٠]

د- القنابل المنطقية **Logic bombs**

تعد نوعاً من أنواع أحصنة طروادة, حيث يزرعها البرنامج داخل النظام الذي يطوره, وقد تكون برنامجا مستقلا , بحيث تعمل عند حدوث أحداث معينة, أو تحت ظروف معينة, أو لدى تنفيذ أمر معين, وتؤدي الى تخريب أو مسح بيانات, أو تعطيل النظام لطرف المستهدف.[٢٧١]

هـ- الأبواب الخلفية **Backdoors**

تمكّن مستخدمي البرامج الخبيثة, من التحكّم في الكمبيوتر المصاب, من خلال إرسال, و استقبال, واطلاق, ومحو ملفات, وعرض بيانات, وإعادة تشغيل الكمبيوتر.وغالبا ما تستخدم الأبواب الخلفية, من أجل توحيد الكمبيوترات الضحية, في مجموعة, لتشكّل شبكة ***بوتنت او زومبي*** ***botnet or zombie*** , تستخدم لأهداف إجرامية سيبرانية.[٢٧٢] وهذا ما يمكن هيئات وأركان حرب المعلومات, من التجوال الحرّ, داخل أي نظام, لأية دولة أجنبية.

و- الرقائق **Chipping**

تحتوي بعض الرقائق الالكترونية, على وظائف غير متوقعة او معروفة,كما في البرامج والنظم, حيث يمكن للدوائر المجمّعة, والتي تشكّل هذه الرقائق, أن تحتوي على وظائف إضافية أثناء تصنيعها, لا تعمل في الظروف العادية, الا أنها قد تعلن العصيان في توقيت معين, او بالاتصال بها عن بعد, حيث يمكن أن تستجيب لتردد معين لبعض موجات الراديو, فتشلّ الحياة في مجتمع, أو دولة ما.[٢٧٣]

---

[270] What is a Trojan Virus? https://usa.kaspersky.com/internet-security-center/threats/trojans#.WA8N1vl9600

[271] Ibid

[272] Ibid

[٢٧٣] عبدالعال، إيهاب عبدالحميد خليفة,استخدام القوة الإلكترونية في إدارة التفاعلات الدولية : الولايات المتحدة الأمريكية نموذجاً خلال الفترة من ٢٠٠١ إلى ٢٠١٢ ,ص:٤٧

ز – مدافع ***HERF***

عبارة عن مدافع تطلق موجات راديو مركّزة, وعالية الطاقة والتردّد, تمكّنها تعطيل وإتلاف أي هدف إلكتروني. أما مستويات الضرر التي قد تحدثها فهي تختلف من ضرر متوسط, كغلق شبكة كمبيوتر,مثلا, أو اعادة تشغيله, الى ضرر بالغ, كإعطاب العتاد الخاص بالكمبيوتر, او الشبكة, بشكل لا يمكن بعده إصلاحهما.[٢٧٤]

ح– قنابل ***EMP***

هي تشبه المدافع, غير أنّها تستخدم نبضات الكترومغناطيسية تمكنّها من التسلل الى مواقع العدو الالكترونية الحساسة, والقاء هذه القنابل, مما يؤدي الى اتلاف كلّ الكمبيوترات, والشبكات، في دائرة انفجارها غير المدوّي, أو المشتعل. وهي أصغر حجما من مدافعHERF, لكنّها أوسع وأبعد أثرا, كما أنها لا تنتقي هدفا معينا, في حين أنّ المدفع HERF ينتقي هدفه.[٢٧٥]

المطلب الثالث: ميزاته

ما يميّز هذه الأسحة استراتيجيا هو ما يلي:

- تجاوزها للقيود الجغرافية, حيث يمكن تنفيذ الهجمات بسرعة البرق, دون الاحتكاك بالخصم في المجال المادي.
- القدرة على العمل بسرية, لجهة القيام بالأبحاث, والتطوير, وتنمية القدرات الهجومية والدفاعية,مما يحمل تحديا حول امكانية السيطرة على هذه الأسلحة مقارنة بالأسلحة التقليدية.
- إمكانية إصابة أهداف استراتيجية, يصعب الوصول اليها عبر الهجوم التقليدي.
- خطورة ضئيلة على حياة السكان.

---

274 **http://hackaday.com/2011/03/21/herf-gun-zaps-more-than-your-dinner/** (last visited september4,2016)

275 خليفة, استخدام القوة الالكترونية وأبعاد التحول في خصائص القوة ,ص:٤٦

- الطابع الانتشاري للفيروسات والذي يمكنها ان تستنسخ نفسها دون توقّف, كما يمكنها من التحرّك داخل الشبكة, في أماكن مختلفة, ما يعطي المهاجم أفضلية على المدافع .
- قدرة تحكّم بشرية عالية, كون الميدان السيبراني مجالاً صناعياً, ومنتجاً بشرياً, ما يساعد على التحكّم والسيطرة, على بيئة ومناخ القتال, مقارنة بالمجال البري, حيث يشكّل الطقس عائقا مؤثراً, على سير الأعمال القتالية.[٢٧٦]

المطلب الرابع: فوائد استخدامه

إنّ الفائدة الكبرى من الأسلحة السيبرانية, بالنسبة لكلّ من **ريد وماكبرني**, تكمن في استخدامها بالتزامن مع الضربات العسكرية التقليدية , كما فعلت اسرائيل مع سلاح الدفاع الجوي السوري عام ٢٠٠٧. كما أن الفائدة الناجمة عن استخدام الاسلحة في الصراع السيبراني, قد تكون أمرا مثيرا للجدل. كما أنهما يتخوّفان من نشوء أسواق للإسلحة الالكترونية. والأسوأ من ذلك, هو ابتكار جراثيم أكثر تعقيدا وحداثة, ما يفسح المجال أمام خلق مشاريع تجارية جديدة. تضاف الى ذلك, مسألة تثير جدلا واسعا يتعلّق بعسكرة الأمن السيبراني. ***فوليام لين William Lynn***, المسؤول الرسمي في البنتاغون, أشار الى أن وزارة الدفاع الاميركية, لن تعسكر الفضاء السيبراني, بقوله: "إن تأسيس قوات دفاع سيبرانية, لا يعني عسكرة الفضاء السيبراني, فوجود القوات البحرية في المحيط, لم يعسكر هذا الأخير".[٢٧٧]

وقد تستخدم الاسلحة السيبرانية, للحصول على المبادأة في ميدان المعركة بوحدات كمبيوترية, كالوحدات الأساسية في القوات المسلحة, وذلك بالإستخدام المتقن لجميع الأسلحة السيبرانية, عبر صراع الكتروني بين القيادات الصديقة والقيادات المعادية, بهدف التأثير على قدرات الخصم, واختراق كيانه الالكتروني, والتي قد تأتي عبر شن الضربات الاستباقية, لمواجهة تهديد محتمل ,والحروب بالوساطة, كأن تبيع احدى المنظمات المتخصصة في الأعمال العسكرية, خدماتها المعلوماتية والأمنية الى بعض الجهات, والحروب السرّية, التي تتخذ طابعا خاصا في الفضاء السيبرانية, لأنها تعتمد على أنواع متطورة من الفيروسات

[276] عبد الصادق,الفضاء الالكتروني والعلاقات الدولية,ص:٢٨١-٢٨٢

[277] Lynn III, W. J. (2011). The Pentagon's Cyberstrategy, One Year Later. *Foreign Affairs*. *https://www.foreignaffairs.com/articles/2011-09-28/pentagons-cyberstrategy-one-year-later*

الالكترونية, اضافة الى هجمات الهاكرز المنسقة, ومعارك المنافسة بين شركات برامج حماية الكمبيوتر, وصناع الفيروسات المعلوماتية.[٢٧٨]

ولتوظيف الأسلحة السيبرانية عسكريا مزايا عديدة, كالتنفيذ بسرعة الضوء, متجاوزة للحدود الجغرافية, دون أي احتكاك بالخصم في المجال المادي. والقدرة على العمل بسرية, فيمكن لمن يستخدم الأسلحة السيبرانية, أن يطورها سرا, دون أن يتم اكتشافه مع القدرة على الاختفاء. كذلك فإن السلاح السيبراني هو سلاح غير قاتل وغير مرئي, حيث تتمكّن الاسلحة السيبرانية أنّ تنفّذ هجوما دون الحاق ضرر مادي بالبشر وبالبنى التحتية, وهذا ما يميزه عن الأسلحة التقليدية, ولكن, في نفس الوقت, يمكن لاستخدامه أن يلحق الأذى بهذه البنى, وبالبشر, عند ضرب الأنظمة المتصلة بالفضاء السيبراني, والموجودة في المجال المادي. وتستطيع هذه الأسلحة, كذلك, أن تصيب أهدافا استراتيجية لا يمكن الوصول اليها عبر الهجوم التقليدي.[٢٧٩]

المطلب الخامس: محدّدات استخدامه

إنّ مدى تأثير الهجوم السيبراني يبقى غير واضح, نظراً لحداثة الحرب السيبرانية, فقد يكون لعمليات سيبرانية تأثير محدود, بينما يكون لأخرى تأثير واسع النطاق.

- من الصعب اعتبار هجوم في الفضاء السيبراني انجازا سياسيا, حيث لا يوجد احتلال لأرض, او لأهداف, كي يتم استخدامها قاعدة لمفاوضات سياسية في مجال الحرب, مثلما يتم فعله في الحرب البرية.
- صعوبة ضمان استمرارية عملية شن الهجوم المتواصل. وفي كثير من الحالات, بمقدور الخصم, أو الطرف المستهدف, أن يسد ثغرات الاختراق, ويستعيد أنظمته بسرعة عالية نسبيا,لإصلاح أضرار الهجوم السيبراني. وهذا ما يؤثر على امكانية تراكم الاضرار, ومن ثم إحداث ضغط سياسي, كما هو الحال, في سلسلة هجما ت جوية استراتيجية.

[278] عبد الصادق,الفضاء الالكتروني والعلاقات الدولية, ص:٢٧٧

[279] المصدر نفسه ص: ٢٩٣

- المخاطر الناجمة عن ردود فعل مضادة, في حالة التعرض للهجوم, والذي من شأنه أن يعرّض الدولة المهاجمة, لضربة مضادة ,ويجتمل أن يأتي الرد, من خارج مجال الفضاء السيبراني.
- إنّ عملية استخدام الهجمات السيبرانية في الصراع الدولي, تحمل خطورة الإضرار بأطراف ثالثة, ليس لها علاقة بموضوع الصراع, كدولة محايدة, او شركة اتصالات دولية, مما يؤدي الى تصاعد ردود فعل من جانب هذا الطرف الثالث.
- يمكن أن تؤدي عملية استخدام الأسلحة السيبرانية, الى مخاطر قيام تحالفات سيبرانية متعارضة, كهجوم روسيا السيبراني على استونيا عام ٢٠٠٧, الذي استنهض حلف الناتو, لضرورة الدفاع عن الدول الاعضاء في المنظمة. فقد ادى الهجوم الروسي الضعيف الأثر الى استنهاض تحالف سيبراني ضدها.
- تمثّل عملية استخدام الهجمات السيبرانية, مخاطر أمام المجتمع الدولي, لاتساع حجم التأثير, وعدم وجود نظام دولي ينظّم العمليات, في مجال الفضاء السيبراني, مع احتمال وقوع خسائر في الأرواح, أو ضرر في منشآت الدولة, وهو ما يعد عملاً عدوانياً وفق القانون الدولي.
- يمكن أن يكشف الهجوم في الفضاء السيبراني, عن القدرات الاستراتيجية للدولة, أمام جميع الأطراف الدولية, مما يعزّز ويسرّع عملية التحصين, والحماية, والخبرة, في مكافحة تلك الهجمات, واحتوائها.
- عدم وجود تعريف واضح للأسلحة السيبرانية, يشكّل نقطة ضعف هامة, في الجهود الدولية, لمكافحة عملية انتشارها, وتطويرها.[٢٨٠]

---

[280] المصدر نفسه, ص:٢٩٤-٢٩٥

المطلب السادس: أهدافه

تتعدّد أهداف السلاح السيبراني, تبعاً لأنواعه. ويمكن تلخيصها على الشكل الآتي:

أ- تشويه المواقع الالكترونية

هو هجوم سيبراني يغيّر من الصفحة الرئيسية للموقع. غالبا ما تكون هذه الهجمات غير مؤذية, وهي غير متبعة من قبل الدول. وكانت المرة التي استخدم فيها هذا الهجوم من قبل دولة, عندما عمد القراصنة الروس, الى تحويل مسار موقع الرئيس الجورجي الى موقع, قورن فيه بأدولف هتلر, وذلك خلال الحرب الجورجية- الروسية, عام ٢٠٠٨.[٢٨١]

ب- هجمات تعطيل الخدمة DDO

أي جعل خدمات الكمبيوتر غير متوافرة, وعبر إغراق الشبكة بالبيانات, وحيث يوجّه ما يسمّى بالكمبيوتر "السيد" ***master***, الكمبيوترات "الزومبيز" ***zombies***, أو "العبيد" ***slaves*** , التي تسلّل اليها الفيروس, لطلب البيانات من مواقع معينة في الوقت ذاته, أو لتحطّيم هذه المواقع أو للتشويش عليها. ومعظم هذه الهجمات, كان مصدرها الصين, وروسيا, وكوريا الشمالية.[٢٨٢]

ج- التجسّس

أي سرقة مخططات الأسلحة. مثالا على ذلك ***Joint Strike Fighter program***, عام ٢٠٠٧, و٢٠٠٨. حيث تمّت سرقة كمية كبرى من البيانات, ومن ثم تشفيرها بحيث اصبح من المستحيل معرفة محتواها. وألمح البنتاغون أكثر من مرة الى تورط الصين بهذا الهجوم.[٢٨٣] ورغم أن التجسّس لا يشكّل عمل حرب وفقا للقانون الدولي, الاّ أنه يعرّض الأمن القومي السيبراني للخطر, وذلك بكشف الخصوم لنقاط القوة والضعف العسكرية, للدول الأخرى. كذلك تمكّن هؤلاء, من زيادة قدراتهم العسكرية, بناء على المعلومات والبيانات, التي تم كشفها. [٢٨٤]

---

281 Clarke and Knake, Cyber War, 16

282 Ibid,p:14

283 Gorman, S., Cole, A., & Dreazen, Y. (2009). Computer spies breach fighter-jet project. *The Wall Street Journal*, *21*. http://www.wsj.com/articles/SB124027491029837401

284 Buijs,the relative power,p:19

د- دخول"الأبواب الخلفية"

إنّ تمكّن قرصان من الدخول الى نظام الكمبيوتر, يجعله قادرا على تغيير الجهاز والبرنامج, قبل وبعد ربطه بالشبكات. فثغرة في عملية التصنيع, تجعل القرصان يدخل "بابا خلفيا", يستخدمه للدخول بسهولة الى الكمبيوتر, أو الشبكة. وقد اعترفت الولايات المتحدة, أنّه تم قرصنة شبكة توليد الكهرباء لديها, وبشكل متكرر ,من قبل قراصنة صينين وروس, تاركين وراءهم قنابل منطقية", قادرة على إغراق البلاد في الظلام, عند تشغيلها, وذلك بنقرة واحدة.[٢٨٥]

---

[285] Electricity Grid in U.S. Penetrated By Spies ,By SIOBHAN GORMAN ,Updated April 8, 2009 **http://www.wsj.com/articles/SB123914805204099085** **(last visited september 6,2016)**

المبحث الرابع: اللاعبون من غير الدول في الفضاء السيبراني

يعد الاهتمام بدراسة اللاعبين من غير الدول في حقل العلاقات الدولية, حديثاً نسبياً, مقارنة بدراسة الدولة. فلقد ظلت الدولة هي اللاعب الرئيسي في تحليل السياسة الدولية, مع تجاهل واضح لتأثير اللاعبين من غير الدول, من الناحية العملية, في قرارات وتفاعلات الدولة, في الداخل والخارج, وذلك يعود الى سيطرة فكر المدرسة الواقعية "الكلاسيكية", على حقل العلاقات الدولية لفترة طويلة, حيث اعتبرت أن الدولة هي الفاعل الرئيسي في العلاقات الدولية, وتجاهلت أي دور للاعبين من غير الدول. حتى الأمم المتحدة, كانت تراها بمثابة أداة, في أيدي الدول.

المطلب الأول: هويتهم

يعرّف قاموس أوكسفورد, اللاعبين من غير الدول, بأنّهم" أفراد أو منظّمات لديها تأثيراً سياسياً هام, ولكن دون تحالف مع أيّة دولة". ويقدّم الاكاديميون, تعريفا آخر, بأنهم "اللاعبون السياسيون المنظمّون, ليس من الضروري أن يكون لهم علاقة بالدولة ,ولكنهم يسعون وراء أهداف, تؤثّر بالمصالح الحيوية للدولة".[٢٨٦]

كما عرّفهم ***وليام دالاس William Dallas***, على أنّهم " منظّمات مستقلة بصورة كبيرة, أو كليّة, عن تمويل الحكومة المركزية, وسيطرتها, وعن اقتصاد السوق, والدوافع السياسية المرتبطة بتوجيه الدولة, وتعمل في شبكات خارج حدود الدولة, التي تنتمي اليها بحكم النشأة, ومن ثم فهي طرف في علاقات متعدية الحدود, تربط بين نظم سياسية واقتصادية ومجتمعات متنوعة, وتعمل بطريقة تؤثر على المشهد السياسي, سواء في دولة ما, أو في منظمة دولية سواء كبعد لنشاطها, أو كغاية رئيسية لها".[٢٨٧]

---

[286] Pearlman, W., & Cunningham, K. G. (2012). Nonstate actors, fragmentation, and conflict processes. *Journal of Conflict Resolution*, *56*(1),*p:2* doi:10.1177/0022002711429669

[٢٨٧] رجب ايمان ،" تأثير الهوية على سلوك الفاعلين من غير الدول فى المنطقة العربية: دراسة حالتى حزب الله وحماس ص١٢

كما عرّفهم البعض, بأنّهم "فاعلون سياسيون منظّمون, ليس لهم علاقة مباشرة بالدولة, ولكن لديهم أهدافهم التي تؤثّر على مصالح الدولة".[٢٨٨]

فهم اذاً, كلّ " اللاعبين, غير الحكوميين, المشاركين في الصراع, ومنهم الإرهابيون, والمعارضون ,والمنظمات الإجرامية, والشركات, والمنظمات المتعددة المصالح, والمجموعات التعاونية المتخصصة, والافراد". [٢٨٩]

المطلب الثاني: تصنيفهم

فقرة أولى: الشركات المتعددة الجنسيات

لقد أصبحت الشركات المتعددة الجنسيات تمتلك موارد للقوّة, تفوق قدرة بعض الدول, ولم يعد ينقصها سوى شرعية ممارسة القوّة, التي ما زالت حكرا على الدول. فمثلاً, إنّ خوادم شركات ***غوغل وميكروسوفت, وأبل*** ,المنتشرة في مختلف دول العالم, تسمح لها بامتلاك قواعد من البيانات العملاقة, وتستطيع من خلالها استكشاف واستغلال الأسواق , بل والتأثير في اقتصاديات كثير من الدول, وإن أرادت, يمكنها التأثير في قوة الدولة الإقتصادية, وقوتها الناعمة أيضا, من خلال تلاعبها بالبيانات والتصنيفات الدولية, للاقتصاديات والأسواق, حيث تتوجّه معظم الدول, الى جذب مثل هذه الشركات الدولية, لخلق استثمارات جديدة فيها, لأن العائد الاقتصادي من تصدير التكنولوجيا مرتفع جدا. فمثلا, نجد أن ثلثي العائد الاقتصادي لشركة أي بي أم ***IBM*** الأميركية, هو من خارج الولايات المتحدة, على الرغم من أن ربع القوى العاملة, والتي تصل الى ٤٠٠ الف موظف, هو من داخل الولايات المتحدة الامريكية والباقي من مختلف دول العالم.[٢٩٠] إنّ هذه الشركات العاملة في الفضاء السيبراني, كيانات تعمل ضمن الاطار القانوني, لأنّ التجاوزات تعرضها لعقوبات اقتصادية ضخمة, أو تعرّض كبار

---

[288] المصدر نفسه,ص:٣

[289] Wilhelmsen, V. C. R. (2014). *SOFT WAR IN CYBERSPACE How Syrian non-state actors use hacking to influence the conflict s battle of narratives* (Master's thesis)..p:14

[290] Lohr, S. (2010). Global strategy stabilized IBM during the downturn. *The New York Times, April, 20*, D1-4(20 April 2010)
http://www.nytimes.com/2010/04/20/technology/20blue.html?_r=0

المسؤولين فيها للمساءلة القانونية. وهذا ما يميّزها عن مجموعات الجريمة المنظمة, علما أنّهما يتشاركان الأهداف نفسها, لجهة السعي لتحقيق الأرباح الاقتصادية, والسيطرة على السوق. هذه الشركات تنشط في الحرب السيبرانية, إما بناء على طلب من الدولة, إما بناء على عقد تجريه مع الدولة, أو تقوم بذلك بشكل مستقل, ولكن ببركة الدولة. ويمكن لوكالات الاستخبارات, أن تضع هذه الشركات في الواجهة, لتغطية لاعمالها الاستخباراتية. إنّ شركات كبرى, تقوم بأنشطة اقتصادية من بلدان عدة, فقد تجد نفسها في وضع محفوف بالمخاطر خلال نزاع سيبراني, مع كلا الطرفين المتنازعين, في الخطوط الأمامية.[٢٩١] ومن أبرز الأمثلة, على قيام الشركات العاملة في مجال الفضاء السيبراني, بالتأثير في العلاقات الدولية, الصراع بين شركة ***غوغل*** والحكومة الصينية, حيث قامت هذه الأخيرة, باختراق حسابات البريد الالكتروني ***Gmail***, الخاصة بالناشطين السياسيين في الصين. كما طالبت شركة ***غوغل***, بحجب نتائج البحث حول الموضوعات التي تعتبرها حرجة, بما يهدّد سمعة غوغل العالمية, خاصة في ظل وجود منافسين أقوياء مثل ***ميكروسوفت***,فضلا عن سعي الحكومة, لسرقة بعض حقوق الملكية الفكرية الخاصة بالشركة. وهذا ما دفع الشركة, الى التهديد بالخروج من السوق الصينية, إن لم تتوقف الحكومة الصينية عن أفعالها.[٢٩٢] يذكر أن هذه الأخيرة, قامت بتطوير محرك بحث ***Baidu*** و ***Sina*** , حتى تستطيع الاستغناء عن غوغل. وأعلنت شركة غوغل, أنّه قد تم حجب جميع خدماتها في الصين بما فيها محرك البحث, وبريد ***Gmail*** , وخرائط ***غوغل***.[٢٩٣]

فقرة ثانية: المنظّمات الإجرامية والجرائم السيبرانية

تعتبر المنظمات الإجرامية, من أهم اللاعبين المؤثرين في التفاعلات الدولية, وهي غالبا ما تلقى حماية من بعض الحكومات. هذه المنظمات, أوجدت لنفسها مكانا على الانترنت, وأصبحت تقوم بعمليات قرصنة الكترونية بهدف سرقة المعلومات, أو اختراق حسابات مصرفية وتحويل الأرصدة منها, أو من

[291] Sigholm, J. (2013). Non-state actors in cyberspace operations. *Journal of Military Studies*, *4*(1),,p:21

[292] Nye, Cyber Power: 13-15

[293] **China Blocks Access to Google's Gmail as Ban Escalates**
https://www.bloomberg.com/news/articles/2014-12-29/china-blocks-access-to-google-s-gmail-as-ban-escalates (last visited september 10,2016)

خلال وجود سوق سوداء على الانترنت, لبيع معلومات مالية متعلقة بكلمات مرور شخصية, وحسابات مصرفية ,وأرقام بطاقات ائتمان, وحيث تكلّف الجرائم الالكترونية الشركات خسائر مالية كبرى.

لقد ازداد عمل هذه المنظمات تعقيدا ونضجا, وهي تعمل على تنويع مشاريعها, باحثة عن مزيد من الأرباح, من خلال الانتقال الى شبكة الانترنت, مكثفة عملياتها حيث البنى القانونية والسياسية ضعيفة, بحيث تستطيع إدارة أعمالها بحرية, ما يدفع المنظّمات المحلية, الى تكييف استراتيجياتها الأمنية, وتقوية عملياتها التجارية الداخلية, مع هذا الوضع. ومن الصعب الكشف عن هويّة هذه المنظمات, لما يتمتّع به الفضاء السيبراني من قابلية للتخفّي, كذلك مراقبتها, وتتبعها من أجل محاكمتها.

فقرة ثالثة: المجموعات الإرهابية السيبرانية

من أبرز اللاعبين الدوليين, الذين ظهروا, لا سيّما بعد أحداث ١١ ايلول, الجماعات الارهابية, حيث استخدمت الانترنت في عمليات التجنيد, والتعبئة, كما استغلت الفضاء السيبراني من أجل نشر افكارها, وجذب المؤيدين والمتطوعين لها, فأصبحت المنصّة الإعلامية, لنشر بياناتها, وتعليماتها لمجنديها. وحتى لو لم يتعدّ الامر لدى هذه الجماعات مرحلة الدعاية والتجنيد, فإنه يظل بإمكانهم اختراق شبكات الكهرباء, والطاقة, والمواصلات, بل المفاعلات النووية, والأسلحة الموجهة إلكترونيا, أو عبر الاقمار الصناعية, والسيطرة عليها أو تدميرها, الأمر الذي قد يسبّب كارثة بشرية. وتعد ممارسة القوة عبر الإنترنت إرهابا, إذا كان لصاحبها دواقع سياسية, كالتأثير في القرارات الحكومية, أو الرأي العام. ويتم ذلك من خلال ثلاثة أبعاد هامة. فالبعد الأول يتمثّل في توفير المعلومات عن الأهداف المنشودة, لتنفيذ عمليات إرهابية تقليدية, وهو مساعد للإرهاب التقليدي, أو وسيط في عملية التنفيذ. أما البعد الثاني, فيستخدم فيه الفضاء السيبراني للتأثير في المعتقدات, مثل التحريض على بث الكراهية الدينية, وحرب الأفكار. أما البعد الثالث, فيتم بصورة رقمية, حيث تقوم الجماعات المتطرفة على اختلاف أشكالها باستغلال مزيا الفضاء السيبراني, من أجل تحقيق أهدافها, في مناطق مختلفة من العالم.[٢٩٤]

ويهدف المهاجمون عبر استخدام الفضاء السيبراني, الى ان يكونوا قوة سيبرانية مهمة, قادرة على إنزال الأضرار النفسية والاقتصادية, لخدمة أهدافهم, ومناصرة حلفائهم. وعلى الرغم من وجود فجوة كبيرة, بين طموحات المهاجمين, وقدراتهم الفعلية على تحقيق هذه الطموحات, فإنّ هذه الفجوة في طريقها للتقلّص,

[294] ايهاب خليفة,القوة الالكترونية وأبعاد التحول في خصائص القوة, ص: ٤٧

خاصة مع التحوّل من عمل فردي لعمل جماعي منظّم, كما أن حدوث تبادل للخبرات والتدريب بين القراصنة, من شأنه تضييق الفجوة الموجودة بين أهداف هذه المجموعات, وقدراتها الفعلية على تنفيذ الهجمات ذات الطابع الفجائي, ويؤثّر ذلك على احتياطات الأمن والحماية, التي تتهدّدها القدرة الهائلة على الحشد والتعبئة, خاصة اذا ما تمّت هذه التعبئة بدافع ديني وإيديولوجي.[٢٩٥]

ويعرّف ***جون سيغهولم Johan Sigholm*** هؤلاء, بأنهم "المتطرّفون الذين لا يتردّدون باستخدام وسائل التطرّف, من أجل القيام بأعمال عنف وحشية تجاه الأبرياء أو الممتلكات العامة, من أجل أهداف سياسية أو عقائدية. فالارهابيون السيبرانيون, هم الإرهابيون الذين يستخدمون الكمبيوتر والشبكات الالكترونية, من أجل تنفيذ هجماتهم, وبثّ الرعب في نفوس الجماهير".[٢٩٦]ويضيف, أنّ الأرهاب السيبراني, كان موضع جدل خلال السنوات الأخيرة, حيث انقسم الخبراء, بين فريق يعتبره على قدر كبير من القوّة والخطر, في العصر الحالي, وآخر اعتبر أنّ الأمر مبالغ به, وهناك مشاكل سيبرانية تفوقه أهمية. حتى أن البعض نفى وجوده, واعتبر أنّ التقارير التي نشرت حول هجمات ارهابية سيبرانية, لا تتعدّى كونها عمليات قرصنة عادية, وأن من يسمّون بالإرهابيين هم لاعبون سيبرانيون عاديون.[٢٩٧]

فقرة رابعة: حركات التحرر الوطني

هم القراصنة الوطنيون, الذين يهدفون الى مساعدة ودعم أوطانهم, التي هي في حالة صراع أو حرب في العالم الواقعي, وذلك من خلال القيام بأفعال تخريبية متعددة, في الفضاء السيبراني, ضد عدوّ الدولة. ويعتبر الرد الذي قام به قراصنة صينيون, على تفجير السفارة الصينية في بلغراد عام ١٩٩٩, واصطدام بين طائرتين عسكريتين تابعتين لكلّ من الجيش الصيني والجيش الأمريكي عام ٢٠٠١ , من الأمثلة الأولى عن القراصنة الوطنيين.[٢٩٨] ولطالما اعتبرت روسيا موطنا للقراصنة الوطنيين, وهذا ظهر جليا خلال هجمات تعطيل الخدمة, ضد استونيا ٢٠٠٧ , وضد جورجيا ٢٠٠٨, وقبلها خلال الصراع في

---

[٢٩٥]عادل عبد الصادق,الارهاب الالكتروني القوة في العلاقات الدولية:نمط جديد وتحديات مختلفة, المركز العربي لابحاث الفضاء الالكتروني مارس ٢٠١٣, الطبعة الثانية,ص:٢٦٣

[296] Sigholm, J. Non-state actors in cyberspace operations. *4*(1),,p:18

[297] Ibid,p:19

[298] Rattray, G. J., & Healey, J. (2011). Non-state actors and cyber conflict. *America's cyber future: Security and prosperity in the Information Age*, *2* p: 72

كوسوفو ١٩٩٩ .[٢٩٩] والأمر نفسه ينطبق على حركتي حماس وحزب الله عام ٢٠٠٠ , حين شنّت مجموعة اسرائيلية, هجمات على موقع هذا الأخير, بعد أسر جنود اسرائيليين, إذ قام فريق من القراصنة, بحذف محتويات موقع حزب الله, ووضع نجمة علم داود وعلم اسرائيل, بدلاً منها. فتم الرد على هذا الهجوم الإسرائيلي, بهجمات مماثلة على ما يقارب ٨٠ موقعا اسرائيليا, أدت الى خروجها جميعا من الخدمة. وفي عام ٢٠١٣ , قامت مجموعة من الشباب باختراق مواقع اسرائيلية, فحصلت على ملفّات سرية, وأسماء أفراد من الجيش الاسرائيلي, ووحدات وأرقام سرّية لبريد الكتروني, وحسابات فيسبوك, وحسابات كثيرة لرجال أعمال اسرائليين, وأكثر من ٥٠٠ مصرف, وتمّ تحميل نحو ألف وثيقة سرية خاصة بالسلطات الاسرائيلية.[٣٠٠]

فقرة خامسة: وكلاء التجسّس السيبراني

إنّ مفهومي الاستخبارات والتجسّس, هما على علاقة وثيقة. فبينما يعتبر العمل الاستخباراتي عملا غير قانوني, تصنّف الكثير من الدول, أعمال التجسّس ضمن نطاق القانون. "فالتجسّس ,يتضمّن الحصول على معلومات حساسة وسرية ,دون إذن صاحبها, ويمكن القيام بها من قبل وكلاء, أو من قبل القوات العسكرية لدولة ما, أو من قبل مؤسسة حكومية, أو قد تقوم بها شركة تجارية, أو منظمة اجرامية, أو حتى الفرد بشكل مستقل".[٣٠١]

ومهما يكن الهدف من التجسّس السيبراني, عسكرياً كان, أم سياسياً, أم اقتصادياً, فالتمييز واجب بين وكلاء التجسّس السيبراني, وغيرهم من اللاعبين كالمجرمين السيبرانيين, بحيث أن وكلاء التجسّس السيبرانيين يعملون وفقا لقانون الدولة, أو بموافقتها ورعايتها. وهناك وجهات نظر, ترى في التجسّس السيبراني, جزءا هاما من المنافسة الاقتصادية العالمية, ومراقبة الإمكانات السيبرانية للخصم, والتي تعتبر ضرورة من ضرورات الأمن القومي.[٣٠٢]

---

299 Ibid.p:16

300 خليفة, القوة الالكترونية وأبعاد التحول في خصائص القوة,ص:٣٩-٤٠

301 Lewis, A ,J.(Sep.-Oct. 2011) "Cyberwar Thresholds and Effects," IEEE Security & Privacy, Volume 9,
Issue 5.

302 Wilson,C."Cyber Crime," in F. D. Kramer, S. H. Starr & L. K. Wentz (eds.),

فقرة سادسة: الفرد كلاعب دولي

لم يقتصر الأمر على المنظّمات والجماعات, بل أصبح للفرد تأثيرا في العلاقات الدولية. ومن أبرز النماذج على هذه الظاهرة ***الوكيليكس wikileaks***, حيث نجح ***وليام أسانج William Assange***, في نشر ملايين الوثائق السرية التابعة لوزراة الخارجية الأميركية, الأمر الذي عرّض الجندي الذي قام بتهريب الوثائق له, للسجن لمدة ٣٥ عاما.[٣٠٣] وفي عام ٢٠١٣ سرّب الموظف السابق لدى وكالة الأمن القومي الأميركية، ***إدوارد سنودن***, وثائق سرية من الوكالة, حول تفاصيل عن برامج تجسس أميركية.[٣٠٤]

ويميّز ***سيغهولم,*** بين القرصان الناشط ***Hactivist,*** وبين القرصان العادي : ***Hacker :***

أولاً: القراصنة الناشطون: وهم يستخدمون الموارد السيبرانية بطريقة قانونية, أو غير قانونية, كوسيلة للاعتراض او للتعبير عن آرائهم الفكرية والسياسية.وقد يستخدمونها بطريقة غير مباشرة, للوصول الى أهداف عسكرية, أو تجارية, أو سياسية غير معلنة. وتعتبر مجموعة الأونيموس ***Anonymous*** , النموذج الأصلي للقراصنة الناشطين. وهم مجموعة من الأفراد, متصلون ببعضهم البعض, من خلال شبكات اجتماعية متعددة (4chan, 711chan forums, Encyclpaedia Dramatica wiki, IRC network) . ومؤخّرا حظوا بانتباه عالمي , نتيجة قيامهم بأعمال سيبرانية على نطاق واسع. من هذه الهجمات, الحرب على الشركات العلمية, والقيام بأفعال سيبرانية لدعم حركات الربيع العربي, والهجوم على شركات تجارية كبرى ***كسوني Sony, ولوي فيتون Vuitton Louis, وماستركارد Mastercard***, ومواقع حكومية امريكية.

ثانياً:القراصنة العاديون: هم أشخاص محترفون في عالم تكنولوجيا المعلومات, وأجهزة وبرامج الكمبيوتر, وبعالم شبكات الانترنت. يعملون بدافع الحشرية, أو التحدي التكنولوجي, أو الربح المادي, أو لأهداف سياسية, أو حتى بدافع الملل. ويقسمهم ***سيغهولم*** الى:

Cyberpower and National Security, National Defense University Press, Washington, D.C. 2009.

[303] خليفة, القوة الالكترونية وأبعاد التحول في خصائص القوة, ص:٤١

[304] قبل "ياهو": هذه أبرز عمليات القرصنة الإلكترونية

http://www.akhbarlibya.net/arabic-news/216982.html (last visited september 21,2016)

أ- **القراصنة ذوو القبعات السود *Black hats*** , ويسمون ايضا ب ***crackers*,** وهم قراصنة يستغلون قدراتهم للاضرار بمصالح الآخرين, أو لتحقيق أهداف غير شرعية, كسرقة البنوك والبطاقات الائتمانية واختراق الهواتف المحمولة ومواقع الانترنت,حيث يتميّزون بقدرتهم على استخدام أدوات الاختراق والقرصنة الالكترونية بهدف السرقة والتدمير والتخريب, ويكثر هؤلاء في ***الانترنت المظلم" Darknet*** .

ب-لقراصنة ذوو القبعات البيضاء *White hats* أو ***Ethical Hackers*** , وهم قراصنة يعملون ضمن القواعد الاجتماعية والاخلاقية. وينشطون من أجل التأكد من أمن المؤسسات وأنظمة المعلومات, وغالبا ما يتم توظيفهم من قبل الحكومات, أو الشركات المتخصصة في أمن المعلومات.

ج- القراصنة ذوو القبعات الرمادية *Gray-hat hackers*, وهم قراصنة يتفقون بالغالب مع القراصنة ذووي القبعات البيضاء, لكن قد يلبسون القبعات السوداء في اوقات معينة, اذا استهدف الهجوم السيبراني مصالحهم. فتارة يقومون بتأمين وحماية أنظمة الكمبيوتر, وتارةً أخرى يقومون باختراقها لتحقيق أهداف شخصية.[٣٠٥]

تستطيع الدول أن تبدأ بسريّة, وتموّل, وتتحكّم, بالهجمات السيبرانية, من خلال قيام اللاعبين من غير الدول بتنفيذ هذه الهجمات بدلا عنها, مخففة من خلال ذلك من التأثيرات السياسية لهذه الهجمات, ومحققة لأهدافها دون عبء الالتزام بأحكام قانون الصراع المسلح. فتوظيف اللاعبين من غير الدول, في عمليات في الفضاء السيبراني, أمر يجذب الدول, لا سيما في سعيها نحو تحقيق اهداف استراتيجية محدودة.

[305] Sigholm, Non-state actors in cyberspace operations ,p:14-15

المطلب الثالث: توظيفهم: ما له وما عليه

يحدّد ***سيغهولم,*** منافع وعيوب توظيف اللاعبين من غير الدول, في الفضاء السيبراني, في النقاط التالية:

فقرة أولى: المنافع

أولاً: يمكن للمهاجم أن يطلق الهجوم السيبراني, في التوقيت المحدد, بوجه الهدف المختار, مستخدما الطرق المناسبة في الهجوم.وقد يحتاج الى كمبيوتر واحد ليدير الهجوم, بينما على المدافع مهمة تحصين موارده السيبرانية بفاعلية, الأمر الذي يرتب عليه أعباء مالية مرتفعة.

ثانياً: يمكن للمهاجم أن يقرر حجم الهجوم, ومدته, لتحقيق التأثيرات المطلوبة.

ثالثاً: إنّ عدم وجود قوانين دولية ملزمة بما يتعلق بالفضاء السيبراني, يخلق ثغرات قانونية تشكّل درعا واقياً للمهاجم, في حال النجاح في اسناد الهجوم اليه.

رابعاً: يمكن للمهاجم اللجوء الى مصادر خارجية, للقيام بالهجمات السيبرانية, كالاستعانة بمليشيات سيبرانية, أو بمجرمين سيبرانيين, او بمتسللين مرتزقة, مع أنّ توظيف اللاعبين من غير الدول بهذه الطريقة, قد يزيد من انعدام الثقة في المجتمع الدولي.

فقرة ثانية: العيوب

أولاً: اذا كانت الهجمات السيبرانية موجهة ضد أهداف مدنية, فالدولة البادئة بالهجوم, ستتهم بارتكابها جرائم حرب, أو برعايتها للإرهاب السيبراني, وبالتالي تصبح منبوذة من المجتمع الدولي.

ثانياً: إنّ توظيف اللاعبين من غير الدول, أمرٌ فيه الكثير من المجازفة, على المدى الطويل. فعلى الرغم أنّ هذه الهجمات قد تكون ناجحة, الاّ أنّه قد لا يمكن الاعتماد عليها. فالمجرمون قد يلجأون الى ابتزاز الحكومة, كي لا تكشف تفاصيل حساسة, ووكلاء التجسس السيبراني المتعاقد معهم, قد ينشقّون وينضمّون الى الدولة الخصم, اذا عرضت عليهم اللجوء السياسي.

ثالثاً: رغم عدم وضوح القوانين المتعلقة بالحرب في الفضاء السيبراني, الا أن الهجمات التي لها علاقة بالدول التي اطلقتها, قد يكون له عواقب سياسية وخيمة. فقد يؤدي التصعيد, الى الانتقام منها بالطرق التقليدية.

رابعاً: قد يجازف المهاجم في التسبب بأضرار جانبية, من خلال ضرب أهداف غير مقصودة. فالهجمات قد تتجاوز حجمها, ومجالها, المقصودين.[٣٠٦]

[306] Ibid, P:26

الفصل الثاني: مجالات توظيف الفضاء السيبراني

على الرغم من أن الفضاء السيبراني يحمل فرصا تجارية, واقتصادية, وثقافية, وسياسية, واجتماعية, وحتى أخلاقية , ولكنه يشكّل مجالاً للتحدّي, وانعدام الامان, وعدم الاستقرار, والجريمة, والمنافسة. فوجود التحديات والفرص, جنباً الى جنب, في معظم مجالات تفاعلات البشر, لهو أمرٌ طبيعي. ولكن الغريزة البشرية تنحو نحو السعي الى الاستفادة من الفرص, أكثر من التحديات, من خلال المراقبة والتنظيم. وهذه الغريزة تقوى في الفضاء السيراني, فيكون الدافع للتنظيم, هو إقناع أو إجبار الحكومات والشركات, على تحسين سلوكهم, في هذا الميدان.

المبحث الأول: تصاعد التنافس الدوليّ

لقد أدّت ثورة المعلومات الى تعدّد أصحاب المصالح من أفراد, ودول, ومجتمع دولي, ورغم أن مشاركة كلّ هؤلاء ضرورية لتحقيق الأمن السيبراني, تبقى الدولة الوحدة الأساسية للمجتمع الدولي. إنّ هناك تمايزات بين الدول, ذلك أنّ الفجوة الرقمية, قد خلقت "عالم الذين يملكون والذين لا يملكون,"[٣٠٧] لجهة ما يسمّى بالثورة التكنولوجية, والتي خلقت تفاوتا بين المجتمعات الغنية والدول ذات الدخل المحدود, وقد تركت آثارا على مسائل الأمن السيبراني, كذلك من خلال عدم التماثل في الموارد والإمكانات هناك. فالدول النامية مهمّشة في الفضاء السيراني, الأمر الذي يضعفها في الفضاء الواقعي, أما البلدان المتطورة, لا سيما صناعياً وتكنولوجياً, فهي في صميمه.

307 OECD High Level Meeting on the Internet Economy, 'Communiqué on Principles for Internet Policy-Making', 28–29 June 2011, p. 2, www.oecd.org/internet/innovation/48289796.pdf.

المطلب الأول الأول: عدم التماثل في الموارد والقدرات

ينعكس عدم التماثل في الموارد والقدرات, في الجوانب التالية:

فقرة أولى: التوزيع الجغرافي لمستخدمي الإنترنت

على الرغم من أنّ أعداد المستخدمين لشبكة الانترنت هو في تزايد مستمر, الاّ أنّ توزيعهم يتفاوت داخل الدول, وبين الدول . فتبعاً لإحصاءات الاتحاد الدولي للاتصالات(ITU), فإنّه, وبالمقارنة مع أمريكا وأوروبا, حيث انتشار الانترنت بلغ ٦٠%, إنّ استخدام الإنترنت في افريقيا, لم يتخط ال ١٠% من مجمل عدد السكان.

فقرة ثانية: الفجوة في المعدّات المتعلّقة بالبيانات الرئيسية

تحتكر شركات أمريكية واوروبية, السوق العالمي لكابلات الألياف الضوئية. ورغم تحوّل بعض الإستثمارات نحو أفريقيا, الاّ أنّ واقع الإحتكار الأوروبي والأمريكي لم يتغيّر. فقد أظهرت الإحصاءات أنه بين عامي ٢٠٠٨ و٢٠١٢ , تم تفعيل أنظمة الكابلات البحرية, بقيمة ١٠ بليون دولار, و كان نصيب المستثمرين الامريكيين والأوروبيين منها, بقيمة ٨٠%. بالمقابل, بلغت إستثمارات القطاع الخاص, من منظمات لا علاقة لها بقطاع الاتصالات, ١٤%, واستثمارات الحكومات, وبنوك التنمية فقط ٥%.كما تشير الإحصاءات, الى أنّ خمس شركات من أمريكا واليابان (HP, IBM, Dale, Oracle and Fuji), استحوذت على ٨٤,٧% من حصص السوق عام ٢٠١٢, ما يعكس سيطرتها على الأسواق العالمية.[٣٠٨]

فقرة ثالثة: الإستفادة العظمى للدول المتقدّمة

تتجلّى في توزيع, وادارة الوسائل المادية للبنى التحتية الرئيسية, التي تؤمّن عمل الفضاء السيبراني. مثالا على ذلك: أسماء النطاقات,[٣٠٩] ١٣منها تديرها ٣ شركات, ٣ منها تتبع لمنظمات حكومية امريكية, و٣

---

[308] Key data elements https://www.ibm.com/support/knowledgecenter/SSS28S_3.0.0/com.ibm.help.forms.doc/Authenticated_Clickwrap/i_authclick_g_key_data_elements.html

[309] **What is Domain Name Resolution** http://www.bleepingcomputer.com/tutorials/what-is-domain-name-resolution/

منها لجامعات أمريكية ايضا, وواحدة لمؤسسة خيرية امريكية , وشركة واحدة ومؤسسة خاصة واحدة في أوروبا, و منظمة يابانية واحدة. والخادم الموزّع الذي يرسل الملفّات اليها جميعا, تمتلكه وتديره مؤسسة أمريكية (VeriSign Inc). هذا التوزيع للبنى التحتية الرئيسية للمعلومات. وغالبا ما يؤخذ هذا التوزيع كدليل لإثبات ما يسمى بالهيمنة على الفضاء السيبراني.[٣١٠]

المطلب الثاني: الفضاء السيبراني: تشادٌّ استراتيجيّ

يشهد الفضاء السيبراني تشاداً بين عددٍ من الدول, أكانت عظمى أم غير ذلك, يعزّز من مكامن القوة كذلك الضعف لدى كلّ منها, كذلك المنطلقات والأهداف. حيث أنّ دولاً عدة في العالم, أخذت تركّز على تطوير قدراتها السيبرانية، ومن أبرزها روسيا, التي يعتبرها مسؤولو الاستخبارات الأمريكية, التهديد الأكبر للولايات المتحدة في مجال الفضاء السيبراني، وكذلك الصين, التي يعد تطوّرها في هذا المجال, جلياً إلى حد كبير. ومن الدول الأخرى المعروف أنّ لديها وحدات ماهرة إسرائيل وفرنسا. ويرى مسؤولو الاستخبارات الأمريكية أن هناك ما يتراوح بين عشرين وثلاثين جيشاً في العالم, لديه قدرات يعتدّ بها في مجال الفضاء السيبراني, مثل تايوان, وإيران, وأستراليا, وكوريا الجنوبية, والهند, وباكستان, والعديد من بلدان حلف شمال الأطلسي (الناتو). فكما قال المدير السابق للاستخبارات الوطنية الأدميرال مايك ماكونيل: «الغالبية العظمى من الدول الصناعية في عالم اليوم لديها قدرات هجومية في نطاق الفضاء الإلكتروني».

ولكن لا يعتمد قياس قوة الدولة السيبرانية, على امتلاك القدرات الهجومية فقط، بل لا بدّ من تقييم عاملين آخرين؛ هما الدفاع والاعتماد. ويُقصد بالدفاع, قياس قدرة الدولة على اتخاذ إجراءات عند تعرّضها للعدوان لصد الهجمة أو تخفيف آثارها، أما الاعتماد, فهو مدى اتصال الدولة بالإنترنت, واعتمادها على الشبكات والأنظمة, التي قد تكون عرضة للأخطار, في حال وقوع حرب سيبرانية.

وعلى الرغم من سرية النشاط المتعلق بالقدرات السيبرانية, إلاّ أنّ التوقعات تشير إلى أنّ هناك ما لا يقل عن ١٢٠ دولة تقوم بتطوير طرق للتجسس, واستخدام الإنترنت, كسلاح لاستهداف أسواق المال, ونظم

---

310 Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review*, *1*(1), 85-86

الكمبيوتر الخاصة بالخدمات الحكومية. ومن أهم الدول التي تمتلك قدرات هجوم إلكترونية, الولايات المتحدة, والصين, وروسيا, وإسرائيل, وفرنسا, وبريطانيا, والهند, وألمانيا.

وعند التفكير في القدرات "الدفاعية" وفي "عدم الاعتماد" معاً, نجد أن كثيراً من الدول, تحرز درجات أعلى من الولايات المتحدة. وهكذا، فإن قدرة تلك الدول على النجاة من حرب سيبرانية بتكاليف أقل، بالمقارنة بما يمكن أن يحدث للولايات المتحدة، تخلق فجوة في الفضاء السيبراني. وقد تغري هذه "الفجوة, دولة ما بشنّ عدوان على الولايات المتحدة. وحيث إنه من المستحيل تقليص الاعتماد على نظم الشبكات اليوم، فالطريق الوحيد لسد الفجوة هو تحسين الدفاعات.

فقرة أولى: الولايات المتحدة الأميركية

منذ حزيران عام ٢٠١٣ انعكست, ممارسات التوسّع الأمريكية للسيادة في الفضاء السيبراني, في المجالات التالية:

أولاً: أعمال مراقبة أعمال الشبكة بحجة ضرورات الأمن القومي والمدعومة من برنامج ***PRISM*** .هذا البرنامج الذي كشف أمره من خلال تسريبات الموظف السابق لوكالة الاستخبارات الامريكية, ***إدوارد سنودن Edward Snowden*** لوسائل الاعلام الأمريكية والأوروبية. ففي حزيران ٢٠١٣, نشرت الواشنطن بوست, مقالا تحت عنوان: "الاستخبارات الأميركية والبريطانية تنقّب عن البيانات من تسع شركات إنترنت من خلال برنامج سري واسع النطاق" كاشفة أن وكالة الأمن القومي الامريكية, قد بدأت بتنفيذ برنامج جمع المعلومات الاستخبارية ***(PRISM)***.[٣١١] و بعد انكشاف أمر هذا الأخير, أعلن المدير السابق لوكالة الامن القومي الأميركية, عن ضرورة جمع المعلومات, بما في ذلك مراقبة البيانات في الفضاء السيبراني, من أجل أهداف الأمن القومي.[٣١٢]

---

[311] **Gellman, B., & Poitras, L. (2013). US, British intelligence mining data from nine US Internet companies in broad secret program**. ***The Washington Post***, ***6***. https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

[312] **Hayden,M.** Ex-NSA chief: Safeguards exist to protect Americans' privacy **CNN Contributor** http://edition.cnn.com/2013/08/01/opinion/hayden-nsa-surveillance/

ثانياً: السعي الى تحقيق أقصى قدر من الحرية للعمليات السيبرانية, لضمان الأمن القومي, بما فيها تبنّي الردع السيبراني, كجزء من استراتيجية الدفاع الوطني. فقد أعلنت الولايات المتحدة الأمريكية, " الحق في الدفاع عن النفس" في الفضاء السيبراني, معتبرة أنّ لها كامل الحق بمهاجمة مصدر التهديد, عندما تجد نفسها معرّضة له. ففي عام ٢٠١٥ وافقت وزارة الدفاع الاميركية, على استراتيجية الدفاع السيبراني, التي تتلخّص بالقدرة على منع, أو السيطرة على التصعيد من كل انواع الصراع من خلال اتباع شبكة من الاساليب" .[٣١٣]

ثالثاً: الحفاظ على حقها السيادي على عمليات ***IANA*** .[٣١٤] ففي آب ٢٠١٥, أعلن مدير الاتصالات والمعلومات في وزارة التجارة الامريكية, عن خطط لتمديد العقد مع أيكان ***ICANN*** , لسنة واحدة, بما يؤمّن ذلك الحق.[٣١٥]

فمن الواضح, اذاً, أن ما تفضّله الولايات المتحدة الامريكية هو توسيع نطاق سيادتها, في الفضاء السيبراني.

وفي عام ٢٠٠٥, صدر عن الأمم المتحدة, تقرير يتعلق بحوكمة الإنترنت, أشار الى أن أنظمة وملفات ***DNS root zone*** , هي تحت سيطرة حكومة الولايات المتحدة الامريكية.[٣١٦] ومنذ ذلك الوقت, بدأت المساعي لإصلاح أسس الحوكمة في الفضاء السيبراني, لترتكّز أكثر على مبدأ المساواة في السيادة, من خلال تحويل صيغ الحوكمة للموارد الرئيسية الممثلة بأنظمة وملفات ***DNS root zone*** . ولكن الاصلاح المذكور بالكاد غادر نقطة الانطلاق. ففي عام ٢٠١٤, عندما تسرّب برنامج

---

[313] The DOD CYBER STRATEGY, The Department of Defense. (2015). http://www.defense.gov/ Portals/1/features/2015/0415_cyber strategy/Final_2015_DoD_CYBER_STRATEGY_for_web pdf

[314] The **Internet Assigned Numbers Authority** (**IANA**) is a department of ICANN, a nonprofit private American corporation, which oversees global IP address allocation, autonomous system number allocation, root zone management in the Domain Name System (DNS), media types, and other Internet Protocol–related symbols and numbers.

[315] Shen, Cyber Sovereignty and the Governance of Global Cyberspace, p: 86

[316] de Bossey, Château. "Report of the Working Group on Internet Governance." *Source: http:// www. wgig. org/ docs/ WGIGREPORT. pdf.(last visit: Dec. 10th, 2016)* (2005).p:5 http://www.wgig.org/docs/WGIGREPORT.pdf

البريزم الامريكي, شعرت الحكومة الامريكية بالضغط مصرحة أنها ستحوّل الاذونات من ***ايانا***, الى القطاع الخاص, متمثلاً ب"مؤسسات أصحاب المصالح المتعددة ". وهي تشمل الشركات, والأفراد, والمنظمات الغير حكومية, حيث القرارات تصدر عن هيئة الإداريين, المؤلّفة من قلّة من المتخصّصين.

واليوم, تعتبر الحرب السيبرانية, من التهديدات الأكثر أهمية التي تواجه الولايات المتحدة الامريكية. وقد تزايد التنبّه لهذا الموضوع, في السنوات الأخيرة, لا سيما في الميدان العسكري. وقد توزّع الاهتمام على مجالات ثلاثةً: الحكومة والجيش والقطاع الخاص. وعلى الرغم من أن الولايات المتحدة اتخذت خطوات هامة, في تمكين الجيش والدفاع في الميدان الحكومي, لكنها عجزت عن وضع ضوابط للقطاع الخاص. وكان كل اقتراح في هذا المجال, يقابل بالاحتجاج بحجّة انتهاك الخصوصية, مما شكّل تحديا ,من الوجهة العسكرية, لأن الكثير من البنى التحتية الحساسة, تقع ضمن نطاق القطاع الخاص.

وتسعى الولايات المتحدة الامريكية, الى الحفاظ على سيطرة استراتيجية,على الميادين القتالية كافة. كما أنها تتخوّف من أن يصبح الخصوم, مساوين لها في الميدان السيبراني, من هنا, تطالب وزارة الدفاع الأميركية, الى زيادة الميزانية المخصصّة للعمليات السيبرانية العسكرية, الى ٦,٧ بليون دولار, في عام ٢٠١٧' أي بزيادة ١٦% عن عام ٢٠١٦. وبرّر وزير الدفاع الأميركي ***أشتون كارتر Ashton, Carter*** طلب الزيادة في الميزانية , بقوله:" يجب أن نتحضّر للمعارك التي قد نواجهها في الأعوام العشرة, أو العشرين, أو الثلاثين القادمة."[٣١٧] وحتى إبّان الأزمة الاقتصادية, والضائقة المالية, التي مرّت بها, لم يتم تخفيض هذه الميزانية.[٣١٨]

والدفاع وحده لا يكفي في الفضاء السيبراني, فلا بد, من أن تشمل العمليات السيبرانية امكانات هجومية. فكما جاء في تحليل صادر عن وزارة الدفاع ," إنّ الدفاعات في شبكة الكمبيوتر, لا يمكن أن تكون, ولن

---

[317] Mccaney,K.(Feb 10, 2016) **CYBER DEFENSE, DOD's $6.7B cyber budget focused on emerging threats**
https://defensesystems.com/articles/2016/02/10/dod-2017-cyber-budget.aspx

[318] Fierce Government IT, 'Panetta: DoD cyber spending won't be cut'
http://www.fiercegovernmentit.com/story/panetta-dod-cyber-spending-wont-be-cut/2012-01-30,

تكون كاملة تماما, فإذا استطاعت وزارة الدفاع الصمود, الآّ أنّها في النهاية ستخضع لهجوم خطير. فكما في الحرب التقليدية, إنّ الهجوم الجيد, هو الدفاع الأقوى".[٣١٩]

لقد كثّفت الولايات المتحدة الاميركية من تركيزها على هذا الميدان, منذ أن جمعت الوحدة السيبرانية السيبركومت Cybercommit , بين امكانيات الجيش, والقوات الجوية, والقوات البحرية, تحت سقف واحد. هذا بالاضافة الى إعلان البنتاغون, عن اطلاقه لاستراتيجية جديدة, تتعلق بالظروف التي تستخدم فيها الأسلحة السيبرانية ضد المهاجمين, معدّدة البلدان التي تشكّل تهديدا كبيرا لها : كالصين وروسيا وايران وكوريا الشمالية. كما أعلنت الولايات المتحدة, عن زيادة في عدد الموظفين من ١٨٠٠ شخص في ٢٠١٤, الى٦٠٠٠ في عام ٢٠١٦. إنّ الهجوم السيبراني الاميركي على البرنامج النووي الايراني عبر استخدام الفيروس ***ستكسنت Stuxnet***,اعتبر أول استخدام للسلاح السيبراني بحق البنى التحتية الصناعية لدولة خصم, حسب ما أورد ***دايفيد سانغر David Sanger***, من جريدة نيويورك تايمز. كما أن إدارة ***اوباما*** صعّدت الهجمات, التي اطلق عليها اسم الألعاب الاولمبية, والتي بدأتها إدارة ***بوش***, كردّ على تخصيب ايران لليورانيوم في موقع ***ناتنز Natanz*** . فلقد قامت الوكالة الأميركية للأمن القومي, بمساندة الوحدة السيبرانية الاسرائيلية السرّية, بتطوير دودة الكمبيوتر, التي أسماها الاميركيون بالحشرة ***the bug***, لتخريب أجهزة الطرد المركزية الايرانية بإخراجها عن نطاق السيطرة, الأمر تم من خلال استغلال نقطة ضعف للكمبيوتر ***سيمنز*** الالماني الصنع, والمستخدم في موقع نتنز, بحيث أدى الى تدمير أكثر من ١٠٠٠ جهاز طرد مركزي في عام ٢٠١٠. ومع اطلاق هجوم ***ستكسنت***, كان على إدارتي ***بوش واوباما,*** أن تزنا المنافع الناجمة عن الإستخدام المسبق للسلاح النووي, في ابطاء البرنامج النووي الايراني. [٣٢٠]

ويقول ***كلارك,*** إنّ من المتفق عليه, اليوم, أنّ الولايات المتحدة, هي الدولة الأقوى, من حيث امتلاك قدرات الحرب السيبرانية.[٣٢١] لكنّ المعضلة الكبرى التي تواجه هذا الدفاع القوي, هي النقص في تحديد الهدف, حيث يصعب عنصر الإسناد للفاعل في الهجمات السيبرانية. فمع بقاء المهاجمين مجهولين, لن تستطيع الولايات المتحدة الرد, وبالتالي لن تستفيد من كلّ القدرات الهجومية التي تمتلكها. كما أن عنصر

---

[320] Sanger, D. E. (2012). Obama order sped up wave of cyberattacks against Iran. *New York Times*, *1*, A1.

[321] Clarke,Cyber War, p:144

سرية الأسلحة السيبرانية, هو مشكلة أخرى تواجه قوة الولايات المتحدة الدفاعية في الفضاء السيبراني , لأن اكتشاف الآخرين لهذه الاسلحة, تدفعهم الى بناء دفاعاتهم حيالها. وقد أدركت الولايات المتحدة, أنّها اذا أرادت ان تحقق ردعا سيبرانيا ناجحا, لا بد لها أن تكشف عن جزء من الغموض, الذي يحيط بنيّتها القيام, ليس فقط بالدفاع بل ايضا بالهجوم في هذا الفضاء. وفعلا, نصّ قانون الدفاع الوطني لعام ٢٠١٢ , على أن "الكونغرس الاميركي يشدّد على امتلاك وزارة الدفاع الامريكية للقدرة, وبناء على توجيه من الرئيس, على شن الهجمات السيبرانية, للدفاع عن وطننا وحلفائنا ومصالحنا."[٣٢٢]

لكن الولايات المتحدة الاميركية, وعلى الرغم من كونها الأكثر تطورا تكنولوجيا, الا أنها الأكثر اعتمادا على أنظمة المعلومات والإلكترونيات, سواءً أكان على الصعيد العسكري, أم على الصعيد المدني. فتوجيه الأسلحة, وتمركز الجنود, وتوجيه الأوامر العسكرية, كلّها تتم من خلال شبكة اتصال إلكترونية. وكلّما ازداد اعتماد الدول على هذه الأنظمة, كلما ازدادت امكانية اختراقها. كما أن البنى التحتية, من مياه وطاقة ومؤسسات مالية, تعتمد ايضا في عملها على الفضاء السيبراني. كما أقرّت الحكومة الأمريكية, بأنّ الاقتصاد والأمن الوطني, يعتمدان على تكنولوجيا المعلومات والبنى التحتية المعلوماتية. كما دعت الى زيادة الاجراءات الأمنية. وهذا الاعتماد, يعني أنّ هجوماً سيبرانياً ناجحاً عليها, ستكون له عواقب كبيرة أكثر من ذلك الذي قد يوجّه على كوريا الشمالية, مثلاً, حيث الإنترنت محدودة الوجود.[٣٢٣]

ولقد أعرب ***لين*** عن اعتقاده, أن " البيتس ***Bits*** و ال ***Bytes***, هي أكثر تهديدا من الرصاص والقنابل في القرن ٢١",[٣٢٤] مشيراً الى أنّ القراصنة, في المستقبل, سيحاولون تدمير الدفاعات الأميركية. والجدير بالذكر, أنّ الدفاع السيبراني العسكري, في الولايات المتحدة الاميركية , منوط بالوحدة العسكرية السيبرانية ***USCYBERCOM***, ووزارة الدفاع ***DOD***, بينما حماية الشبكات الحكومية, وشبكات القطاع الخاص, هي ضمن اختصاص وزارة الداخلية.

322 House of Representatives, ‘National Defense Authorization Act for Fiscal Year 2012’, 629. http://www.rules.house.gov/Media/file/PDF_112_1/legislativetext/HR1540conf.pdf

323 DHS, ‘National Strategy to Secure Cyberspace’, viii and 6

324 **Brookes, A. (2011). US Pentagon to treat cyber-attacks as ‘acts of war. BBC News, 1.** http://www.bbc.com/news/world-us-canada-13614125

ولا تزال الولايات المتحدة, تعاني من مشكلة إسناد الفعل. ورغم تطويرها لتقنيات تساعدها في هذه المهمّة, الا أنّها بحاجة الى المزيد من التمويل. فالردع أوالهجوم السيبراني الأميركي, لا يمكن أن يصل الى قوته الكاملة, بسبب هذه المشكلة. وتبعا لهذا الغموض في الأمن السيبراني, إنّ قوة أمريكا في هذا الميدان, هي من النوع المتوسط. وهناك ميل الى اعتبار قوتها السيبرانية في تناقص.[٣٢٥]

Nation	Cyber Offense	Cyber Dependence	Cyber Defense	Cybersecurity total
United States	Very high	Very high	Low/Medium	Medium

Table 2 - Adapted from: Clarke, Cyber War

فقرة ثانية: الصين

منذ عام ٢٠١٣, أصبح الأمن السيبراني, من المواضيع الأكثر أهمية في أجندة الاستراتيجية الكبرى, للأمن القومي الصيني, لاسيما بعد تأسيس مجموعة جديدة, تحت قيادة الرئيس الصيني مباشرة , وذلك لمواجهة التحديات والتهديدات السيبرانية. وكان الهدف بناء قوة سيبرانية, تحوّل الصين من لاعب في الفضاء السيبراني, الى قوة عظمى فيه.[٣٢٦] هذا يعني, أن الصين ستعمل, ليس فقط على استراتيجية الدفاع في الفضاء السيبراني, بل ستصبح أكثر تأثيرا, في وضع القواعد التي تحكم هذا الفضاء. وتحتل السيادة السيبرانية موقعا مركزيا في استراتيجية الأمن السيبراني, حيث حماية السيادة واحدة من المهام المطلوبة لضمان الأمن القومي, والمدرجة في قانون الأمن الوطني الصيني. كذلك هو الهدف الرئيسي لقانون الأمن السيبراني الصيني, وقد نصّ على أنّ حماية السيادة في الفضاء السيبراني والأمن القومي, هما السبب لوضع هذا القانون.[٣٢٧] والمنطق نفسه ينطبق ايضا على المناقشات الدائرة حول وضع قواعد جديدة لإدارة الفضاء السيبراني. فالصين لا تثق بمقاربة " تعدد أصحاب المصالح" التي تفضلّها الحكومة الأمريكية, على اعتبار ان هذه الاخيرة, تسيء استخدام صلاحياتها فيها, لتوسّع سيادتها هناك, وتستخدم هذه المقاربة, كعذر لتجنب مواجهة الدول الأخرى, كالصين, حماية لمصالحها في الفضاء السيبراني.[٣٢٨]

---

325 Buijs,the relative power, p:40

326 **Xi Jinping leads Internet security group**
http://webcache.googleusercontent.com/search?q=cache:http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm

327 Shen, Cyber Sovereignty and the Governance of Global Cyberspace, p:90

328 Ibid, p:91

لقد ورد في التقرير السنويّ لوزارة الدفاع الاميركية, المقدّم الى الكونغرس والمتعلّق بالصين, أن هذه الأخيرة ,أعلنت للمرة الأولى, أن الفضاء السيبراني هو" ميدان جديد للأمن الوطني ومجال للمنافسة الاستراتيجية". كما جاء في التقرير, أنّ الصين ترى أنّ قدراتها السيبرانية تخدم ثلاث نقاط:

- السماح لجيش التحرير الشعبي, بجمع البيانات للاستخبارات والعمليات السيبرانية الهجومية(ويرى التقرير أن هذه النقطة هي الهدف الاهم).
- إعاقة الاجراءات, او إبطاء الرد عبر استهداف الاتصالات, والنشاطات التجارية المتصلة بالشبكة.
- مضاعفة القوة, ومساندة الهجمات العسكرية خلال الصراع أو الأزمات.

ولكن التقرير أشار الى أن الصين تقوم بحشد طاقاتها, لتطوير قوّة سيبرانية شبيهة بما قامت به الولايات المتحدة, بشأن إنشاء الوحدة السيبرانية, وذلك للتعامل مع ما تراه تهديداً سيبرانياً متصاعداً. هذه الخطوة, هي مثال آخر عن تنامي الفضاء السيبراني, كجزء من العمليات العسكرية [٣٢٩].

أما بالنسبة لقرصنة بيانات مكتب إدارة شؤون الموظفين الاميركي, وبالرغم من أن الادارة الاميركية نسبت عمل القرصنة هذا الى الصين, الاّ أنّها لم تظهر ذلك الى العلن. هذا الاختراق أثّر سلبا على البيانات الشخصية ل٢٢ مليون موظف حالي وسابق, في الحكومة الاميركية, وكشف عنه في حزيران عام ٢٠١٥. هذا التحفظ الاميركي, في تسمية الصين كمتهم بالهجوم , كان سببه قلقاً امريكياً من أنّ هذا الامر , سيتطلب بالمقابل من امريكا, الكشف عن تفاصيل تتعلق بقدراتها السيبرانية, وبعمليات تجسّس تقوم بها. فوفقا لجريدة ***الواشنطن بوست***, أعرب مدير الاستخبارات الوطني **جيمس كلابر** ***James R. Clapper*** , وعلى مضض,عن إعجابه بالاختراق قائلا, إنّ على وكالات التجسس الاميركية القيام بالأمر نفسه ضد الحكومات الاخرى.[٣٣٠]

وقد استنتجت دراسة أمريكية, أنّ الصين تعمل مع قراصنة مدنيين, على تطوير قدراتها السيبرانية الهجومية, رغم صعوبة إثبات ذلك. كما ينظّم الجيش الصيني مبارايات قرصنة, ويخصص مكافآت

---

[329] Dod report on China details escalation in the cyber domain
https://defensesystems.com/articles/2016/05/16/dod-report-china-cyber-domain.aspx

[330] Nakashima, E. (2015). US Decides against Publicly Blaming China for Data Hack. *The Washington Post*.

للرابح , للتأكد من قدرات الصين البشرية في هذا المجال, وامكانية توظيفها.[٣٣١] حتى أن ***جايمس مالفنون*** ***James Mulvenon***, وهو باحث متخصص في الشؤون العسكرية الصينية, يتحدث عن منظمة قراصنة وطنيين, تستخدمها الحكومة, للقيام ب"العمل الوسخ عنها". [٣٣٢]

فقوّة الصين الهجومية إذا هي أكثر فاعلية, لأنها تعتمد على استخدام القراصنة المدنيين, الأمر الذي يسهّل عليها إمكانية إنكار تورطها, في حال تم النجاح بإسناد العمل الى مهاجم محدّد. هذا مع العلم أنّ المدافعين يكونون على علم بوقوف الحكومة الصينية وراء الهجوم, بسبب الموارد والاستخابارات اللازمة لتنفيذه, بالاضافة الى كون هذا الأخير, مركّزاً على أهداف عسكرية.[٣٣٣] وبالرغم من أنّ الأسلحة السيبرانية التي تستخدمها الصين, أقل تعقيدا من الأسلحة الأميركية, فإن مشكلة الإسناد التي تضعف الموقف الدفاعي الأمريكي, تستفيد منها الصين. وهذا الأمر يدفعها الى إطلاق هجماتها, دون الخوف من أن يتم الامساك بها, مما يجعل الأسلحة السيبرانية الصينية, تصل الى مستوى قوة نظيرتها الأميركية.

وتعتبر الصين أقل اعتمادا من الولايات المتحدة على أنظمة المعلومات, سواء من الناحية العسكرية أم المدنية. فنظام توليد الكهرباء لديها مثلا, لا يزال يتم التحكم به يدويا, مما يجعله أقل تأثرا, فيما لو تعرض لهجوم سيبراني. كما أن نسبة إختراق شبكة الإنترنت لديها, أقل مما تتعرّض له الشبكة الأمريكية, وذلك لأنّ عدد مستخدمي الشبكة, هم تقريبا ما يعادل نصف عدد السكان (تبعا لإحصاء البنك الدولي لعام ٢٠١٦, أي هناك ما يقارب ال٧٠٠مليون مستخدم). كما أنّ الجيش الصيني, لا يزال يعتمد على الأسلحة التقليدية, والتفوّق العددي, أكثر من اعتماده على الأسلحة الالكترونية. ولكن, وعلى الرغم من أنّ الصين تتجه, اليوم, نحو وضع أهداف لزيادة دمج اقتصادها, وصناعاتها, وتقنياتها العسكرية بأنظمة المعلومات, الاّ أنّها تحاول أن تبقي زمام الأمور تحت سيطرتها, قدر الإمكان.

وبالنسبة لها, إنّ حماية الفضاء السيبراني, مسألة دفاع قومي. هذا يعنى أن الحكومة تتحكّم كليّا بهذا الفضاء, وتمارس الرقابة عليه, لا بل تفصل شبكة الانترنت الداخلية عن العالم الخارجي ,أو تعطّلها

---

331 Elegant, S. (2007). Enemies at the Firewall. *Time Magazine*, *6*. http://www.time.com/time/magazine/article/0,9171,1692063,00.html,

332 Segal, A. (2012). Chinese computer games: Keeping safe in cyberspace. *Foreign Aff.*, *91*, 14. https://www.foreignaffairs.com/articles/china/2012-03-01/chinese-computer-games

333 Clarke, Cyber War, p:147

نهائيا. ويقول ***كلارك,*** إن الانترنت في الصين تعمل كشركة انترنت داخلية, حيث الدولة هي مزوّد الخدمة لكل مستخدم لشبكة الإنترنت, وبالتالي لها السلطة المطلقة للتحكم بهذه الشبكة. كما أنّ مسؤولية الدفاع تقع على عاتق جيش التحرير الشعبي الصيني PLA, وليست مقسّمة المهام بين وكالات متعددة ووزارات, كما هي الحالة الأمريكية. وتسعى الصين, الى تشكيل وحدة سيبرانية, شبيهة بالسيبركوم الأميركية, لتقوم بالمهام الدفاعية السيبرانية فقط. وما يساهم في تقوية الدفاع السيبراني الصيني, هو القدرة على اتخاذ القرارات, وتنفيذها بالسرعة اللازمة, دون جدال يتعلق بالتمويل والموازنة. حتى أنّها وضعت تشريعات سيبرانية, مكّنتها من أن تحصّن البنى التحتية السيبرانية, بما يسمى جدار النار الصيني العظيم ' the Great Firewall of China'[٣٣٤]. وعلى الرغم من سيطرة الحكومة الصينية على الانترنت المحلي, الا أن اعتمادها على برامج القرصنة, يزيد من هشاشة دفاعها السيبراني جاعلا الأمن السيبراني الصيني في الدرجة المتوسطة.

Nation	Cyber Offense	Cyber Dependence	Cyber Defense	Cybersecurity total
China	High	Medium/High	Medium	Medium

Table 3 - Adapted from: Clarke, Cyber War

فقرة ثالثة: روسيا

نشر الموقع الالكتروني الإخباري المستقلّ, ***مدوزا Medoza***, عشية الإنتخابات الأميركية,[٣٣٥] تقريرا مفصّلا عن كيفية بناء روسيا لأكبر جيش سيبراني. وأكثره عدائية في العالم,في الوقت الذي يتهم فيه المسؤولون الرسميون الامريكيون روسيا بمحاولة التأثير على نتائج التصويت, من خلال القرصنة, وتسريب البريد الالكتروني, لإلحاق الضرر بمرشّحة الحزب الديمقراطي, ***هيلاري كلينتون***. هذا و يدّعي خبراء الأمن السيبراني, أن روسيا تتدخّل في الشؤون الاوروبية منذ سنوات. كما يشير التقرير, الى أن روسيا توظّف قراصنة ومجرمين, وتختبر قدراتها السيبرانية على دول شرق أوروبا, قبل أن تحوّل انتباهها الى الولايات المتحدة الاميركية, هذا العام. وأعتبر التقرير, أن وزارة الدفاع الروسية, ركّزت جهودها على

334 Betz & Stevens, *Cyberspace and the State*.p:71

335 **New Report Lifts Curtain On Russia's Construction Of Powerful "Cyberarmy"** https://www.buzzfeed.com/sheerafrenkel/new-report-lifts-curtain-on-russias-construction-of-powerful?utm_term=.spNWyAn7BB#.tawwL58edd

توظيف أكاديميين, وقراصنة ذوي خلفيات إجرامية, على حد سواء, في المؤسسة العسكرية. كما طوّرت أسلحة سيبرانية هجومية, واشترت أدوات من شركات أمن سيبرانية للمراقبة والتجسّس.

إنّ تورّط الحكومة الروسية في العمليات السيبرانية, ليس جديدا بل يعود الى عام ٢٠١٢, مع إعلان وزير الدفاع الروسي في تصريح رسمي عن الحاجة الى وحدة سيبرانية, تحاكي الوحدة السيبرانية الأميركية. وفي عام ٢٠١٤, أسّست وزارة الدفاع مركزا للدراسات الخاصة, وبدأت بتعيين أشخاص, تم انتقاؤهم من مواقع وصفحات الكترونية لجامعات الهندسة الروسية. كما استدعت خبراء متخصّصين في برامج هجوم سيبرانية, مقدّمة لهم الحماية الأمنية, ورواتب مالية عالية. وأسّست فرقة بحث ضمن الوحدات العسكرية الروسية. هذا ويشير ***ديمتري البيروفيش*** ***Dmitry Alperovish*** (الباحث لدى شركة ***كراودستريك*** ***Crowdstrike***, وهي شركة أمن سيبرانية امريكية) الى أن لروسيا تاريخا حافلا, في إرغام القراصنة على العمل مع الحكومة, لتجنّب السجن.

وعلى غرار الصين, فإنّ روسيا تستفيد من ثغرة في عنصر إسناد الفعل, لأنها تعمل في المساحة الرمادية بين الدولة والأفراد, في الفضاء السيبراني. فالهجمات السيبرانية التي نسبت الى روسيا, تظهر أنها تمتلك قدرات هجومية سيبرانية, هامة تصنّفها من متوسطة الى عالية.[٣٣٦]. ويصل معدل الروس الذين يستخدمون شبكة الانترنت, اليوم, الى ٤٢% من مجموع السكان. [٣٣٧] وهناك ايضا نمو متسارع, نحو زيادة اعتماد روسيا على الفضاء السيبراني . فالمدن الضخمة كموسكو وسان بيترسبرغ اصبحتا متصلتين بالشبكة, بنسبة استخدام تفوق ال ٧٠% . أما عسكريا, فلقد طوّر الجيش شبكة عسكرية تكتيكية, لتسهيل استخدام التقنيات السيبرانية, في ساحة المعركة. لكن, يبقى أنّ اعتماد روسيا على الفضاء السيببراني, أقل من نظيرتها الأمريكية . ويشير تقرير صادر عن برنامج الأمن والدفاع الروسي, أن الفضاء السيبراني لم يطاول كلّ البنى الحكومية الروسية بعد, ما يجعلها أقل تأثّراً بالهجمات السيبرانية اذا ما وقعت.[٣٣٨]

[336] Buijs,Relative power,p:50

[337] **With 84 million users, Russia's Internet penetration rate has nearly doubled in five years** ,http://www.ewdn.com/2016/02/08/with-84-million-users-russias-internet-penetration-rate-has-nearly-doubled-in-five-years/

[338] SDA, 'Cyber-security',P: 77

ولكن " العدوان الايديولوجي" مقلق للروس, أكثر من التجسّس أو التخريب في الفضاء السيبراني, أي استخدام الإنترنت لتشويه سمعة حكومات الدول الأخرى. ومن هنا, فهي تدعو الى قوننة دولية لهذه المسألة, من خلال الأمم المتحدة. فروسيا لا تعطي أهمية للخطر الناجم عن الأسلحة السيبرانية , حيث إنّها تكرّس مواردها لمحاربة الدعاية أكثر من ايلائها الإهتمام لمحاربة التدخلات الغير مرغوب فيها. وهذا يظهر جلياً, في سعيها البطيء الى تطوير دفاعاتها السيبرانية. كما أن محدودية التشريعات, التي تنظم استخدام شبكة الانترنت في روسيا, بالمقابل, تزيد من ضعف الدفاع السيبراني الروسي. واعتماد روسيا على قراصنة شبكة الأعمال الروسية ***RBN*** , جعلها أنشط في مجال الهجوم, منه في الدفاع ,نظرا لقدرات هؤلاء المركّزة, على خلق الأسلحة السيبرانية, أكثر من مهارتهم في الدفاع السيبراني.[٣٣٩] ولكنّ قوة روسيا الدفاعية في الفضاء السيبرانية تكمن في شبكتها الداخلية, حيث بإمكانها مراقبة المستخدمين بسهولة, إضافة الى صعوبة خرقها.[٣٤٠]

اذاً روسيا متأخّرة نسبيا في الدفاع السيبراني, وتشريعاتها غير كافية. كما أنّ الجيش متأخّر في الميدان التكنولوجي كالحرب المركزة ***Network centric warfare*** . وفيما يتعلق بالأمن السيبراني فإنّها تعطي أولوية للتركيز على الجهمات المعلوماتية, التي تؤثّر على رأي الجماهير. والخلاصة, فإن الأمن السيبراني لروسيا, هو من الدرجة المتوسطة وفقا للجدول التالي:

Nation	**Cyber Offense**	**Cyber Dependence**	**Cyber Defense**	**Cybersecurity total**
Russia	Medium/High	Medium	Low	Medium

Table 4 - Adapted from: Clarke, Cyber War

لقد اتهمّت روسيا باستخدام الأسلحة السيبرانية, لتنفيذ هجوم ضد كلّ من استونيا وجورجيا., حيث كانت هذه الأخيرة في ربيع ٢٠٠٧ , هدفا ل"هجوم تعطيل الخدمة" الذي أغلق بالقوّة مواقعها الإلكترونية, وغيرها من منصّات الشبكة الإلكترونية. وقد أثقل الهجوم الحمل على الخوادم , وحطّم المواقع الالكترونية للبرلمان الاستوني, والوزارات, والمنظمات السياسية, والجرائد, والمصارف. هذا الهجوم, والذي كان عملا تخريبيا, أكثر من كونه تدميريا, استخدم البوتنت ليغرق المواقع الالكترونية بها. وكان الدافع قرار الحكومة الاستونية, بتغيير مكان تمثال يعود للحقبة السوفيتية في ذكرى الانتصار على المانيا

339 Buijs,the relative power P:51

340 Ibid, p:77

النازية. وقد اتهمت الحكومة الاستونية علنا روسيا, بالقيام بهذا الهجوم, مع أنه أسند الى ناشطين وطنيين روس, لكن لم تثبت أية علاقة محددة بينهم وبين الحكومة الروسية. وكان هذا العمل, قد وصف بأنه"عمل شغب سيبراني أكثر منه هجوما سيبرانيا". كمااستبعد مسؤول رسمي سابق في الأمن السيبراني الاميركي, الدولة كلاعب في هذا الهجوم .[٣٤١] وقد كرّر الأمر في اختراق روسي للمواقع الالكترونية للحكومة الجورجية, والاعلام الجورجي عام ٢٠٠٨, لكنّ بنى الدولة التحتية لم تتعرّض للتخريب. وقد أسندت الحكومة الجورجية هذا الهجوم الى روسيا, لأنه سبق مباشرة الغارة التي شنتها هذه الأخيرة على الحدود الجورجية, بدعم من الانفصاليين في ابخازيا واوستيا. لكن تحليلات تلت,لم تستطع اثبات علاقة مباشرة بين "القراصنة الوطنيين" الروس, الذين أطلقوا الهجوم السيبراني, وبين الحكومة الروسية.

ويذكر أنه عام ٢٠١٤, تمّ توجيه اتهام الى روسيا حول هجوم سيبراني, على شركة الاتصالات الاوكرانية ***اكرتلكوم Ukrtelecom*** , نظرا للمهنية السيبرانية العالية التي تملكها من جهة, ولكون معظم البنى التحتية لهذه الشبكة, قد انجزت عندما كانت جزءاً من الاتحاد السوفياتي, حيث تلاعب قراصنة بكابلات الألياف الضوئية للشركة, متسببن بانقطاع الاتصالات الهاتفية, وتعطيل شبكة الانترنت.

فقرة رابعة: كوريا الشمالية

يعتقد أن كوريا الشمالية, هي وراء عدد هام من الهجمات, كتلك التي وجّهت مؤخرا الى شركة ***سوني Sony***. ووفقا للمسؤولين الرسميين الاميركيين, إنّ كوريا الشمالية شاركت بصورة أساسية, في قرصنة كمبيوترات شركة سوني, لسرقة بياناتها عام ٢٠١٤. هذا الفعل تسبّب بإحراج أكثر مما تسبب باضرار (نشر رسائل بريد الكترونية, وتسريب معلومات عن الرواتب, وعرض أفلام لسوني لم تطلق بعد). وقد شكّل هذا الهجوم, رد فعل على محاولة لإفراج وشيك عن فيلم كوميدي يسخر من الرئيس الكوري ***كيم يونغ اون Kim Jong Un*** . وكان مكتب التحقيقات الفدرالي, قد استطاع أن ينسب الهجوم السيبراني الى كوريا الشمالية, بسبب جهود هذه الأخيرة لاخفاء أثر الأدلة. وكانت الإدارة الأميركية, قد قامت ب"رد متناسب", من خلال فرض العقوبات على عشرة مسؤولين كوريين رسميين, بتهمة "التورّط في الكثير من

[341] Waterman, S. (2007). Analysis: Who cyber smacked Estonia?. *UPI. com.*

العمليات السيبرانية الرئيسية".[٣٤٢] وواكب الرد الفعل الرسمي عملية سرية, أنكرتها الحكومة الاميركية , وهي القطع المؤقت لشبكة الانترنت عن كوريا الشمالية. وقد طلبت الإدارة الأميركية من حكومة بكين, المساعدة في تعطيل قدرة النظام الكوري, على الاستمرار في الهجمات السيبرانية, بسبب اعتماد هذه الأخير عليها, للوصول الى شبكة الانترنت. [٣٤٣]

فقرة خامسة: ايران

في ما خصّ إيران, إنّ قدراتها السيبرانية في تطوّر متزايد, ويعتقد أنها وراء العديد من الهجمات في المنطقة. ففي عام ٢٠١٢ , قام قراصنة ايرانيون بهجوم على الشركة السعودية النفطية ***ارامكو***, متسببّين تقريبا, بمحو البنية التحتية لتكنولوجيا المعلومات الخاصة بالشركة, والتي كانت على وشك الانهيار.[٣٤٤] فلقد دمّر الفيروس الذي سمي ***بشامون Shamoon*** , الأقراص الصلبة لثلاثين الف كمبيوتر.[٣٤٥] وتكمن وتكمن أهمية الحدث, في حقيقة أنّ هذه البرمجيات الخبيثة, كانت معدة لتخريب أكبر عدد ممكن من الأجهزة, في شركة معنية ببنى تحتية حساسة. وقد اعتبر وزير الدفاع الأميركي ***Leon Panetta ,*** فيروس شامون "كأداة معقدة",[٣٤٦] بينما وصف باحثون اخرون من مركز ***كاسبرسكي Kaspersky Lab*** , والمعنى بتطوير البرمجيات المضادة للفيروسات, أخطاء الترميز التي اعترت التعليمات البرمجية,

---

342 Schmidt, M. S., & Sanger, D. E. (2015).“More Sanctions on North Korea After Sony Case,” New York Times.http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html

343 Fackler, M. (2014). North Korea Accuses US of Staging Internet Failure. *The New York Times*, *27*.
http://www.nytimes.com/2014/12/28/world/asia/north-korea-sony-hacking-the-interview.html

344 Perlroth, N. (2012). In Cyberattack on Saudi firm, US sees Iran firing back. *New York Times*, *23*. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

345 Higgins, K. J. (2013), “The Long Shadow of Saudi Aramco,” Dark Reading http://www.darkreading.com/attacks-breaches/the-longshadow-of-saudi-aramco/d/d-id/1140664?

346 Stewart,P.(2012) “Shamoon Virus Most Destructive Yet for Private Sector, Panetta Says,” Reute. http://www. reuters.com/article/2012/10/12/us-usa-cyber-pentagon-shimoonidUSBRE89B04Y20121012

بمثابة عمل هواة, وأن البرنامج الخبيث, كان يمكن له أن يكون أكثر دماراً.[347] فالمهاجمون أرادوا الاستفادة من الرقابة الضعيفة, خلال فترة الأعياد لدى المسلمين, ما سمح للفيروس أن ينتشر. وأثّر الهجوم على إنتاج النفط, والأعمال التجارية للشركة, بسبب فقدان بيانات تتعلّق بالتنقيب والانتاج. وقد تطلب الأمر من الشركة عشرة أيام لاستبدال الأقراص الصلبة المتضررة.[348] وبالرغم من أنّ مجموعة ناشطة, تبنّت مسؤوليتها عن الهجوم, معلنة أنّه رد فعل على سياسات المملكة العربية السعودية في الشرق الأوسط, فإنّ كثيرين, ومنهم مسؤولون في الحكومة الأميركية شكّكوا في تورّط الإيرانيين.[349]

المطلب الثالث: عسكرة الفضاء السيبراني

تتجّه الدول اليوم لتعزيز دفاعاتها ضد خطر التعرّض للهجمات السيرانية, لكن الإتجاه الأخطر, هو التحوّل من اتخاذ اجراءات وقائية ذات طابع دفاعي, الى الاتجاه نحو تبنّي سياسات هجومية, ويلعب التسليح أهمية استراتيجية في توازن القوى, وبسط النفوذ, وتمكين الدول من ممارسة العديد من الأدوار, والضغوط, والتكتلات في ظل بيئة يمتلكها الشك وعدم اليقين, وهو ما يحمل خطورة لجهة عسكرة الفضاء السيبراني, دون الأخذ بعين الاعتبار, كونه يختلف عن ظروف التقدم في امتلاك الاسلحة النووية, أو البيولوجية, ودون حجم التدمير المنتظر وقوعه, حال التعرّض لهجوم سيبراني.

ولكن عند دخول العالم سباق التسلح السيبراني, تبرز مشكلتان: الأولى, هي تحديد ماهية الأسلحة التي يمتلكها الآخرون ليتمكّن المجتمع الدولي من التدخّل لاحتواء التقدّم في مجال تلك الأسلحة. والثانية, في

---

347 Fahmida,R.Y.(2012) "Coding Errors in Shamoon Malware Suggest It May Be the Work of Amateurs," Security Week
http://www.securityweek.com/coding-errors-shamoon-malware-suggest-it-may-be-work-amateurs

348 Roberts,P.(2012) "Whoddunnit? Conflicting Accounts on Aramco Hack Underscores Difficulty of Attribution," Naked Security
http://nakedsecurity.sophos.com/2012/10/30/whodunnit-aramco-hack/

349 Gorman, S., & Barnes, J. (2012). Iran Blamed for Cyberattacks. *The Wall Street Journal*.
http://www.wsj.com/articles/SB10000872396390444657804578052931555576700

مجال التفتيش, كآلية المراقبة للأسلحة النووية. ومن الأهداف التي تسعى اليها الدول من خلال بنائها لقدراتها العسكرية في مجال الأسلحة السيبرانية , ما يلي:

- تحقيق التفوق التقني من خلال امتلاك التكنولوجيا , وأنظمة الحماية , وتطوير القدرات الهجومية.
- مواجهة الهجمات السيبرانية, من خلال اختبار الدولة لمدى جهوزيتها. أو من خلال التطوير الذاتي للقدرات الهجومية, أو من خلال الاستعانة بأفراد أو بشركات متخصصة.
- توفير الميزانيات المخصصة لتطوير القدرات الهجومية, والدفاعية, للدولة, كونها أقل تكلفة مما تنفقه على الجيوش

وبعد الهجمات السيبرانية التي قامت بها الولايات المتحدة وغيرها من الدول انطلق سباح تسلح رقمي محموم مسببا عدم الاستقرار ,حيث تقوم الدول بحشد مخزونها من الشيفرات الخبيثة . فانتشا ر هذه الاسلحة, توسّع الى حد أن خصمين سيبرانيين, كالولايات المتحدة والصين, قد اتفقتا عام ٢٠١٥,على وضع معايير ضد الهجمات السيبرانية, التي تشن بين بعضها البعض, خاصة تلك التي تحصل من قبل الصين على الشركات الخاصة, بهدف سرقة الملكية الفكرية, او الأسرار التجارية, أو معلومات سرّية لغايات تجارية. وكان ***دانيل راسل Danielle Russel***, مساعد وزير الخارجية لشوؤن شرق آسيا والمحيط الهادئ, قد حذّر من أن الفضاء السيبراني, لديه القدرة على زعزعة الثقة في العلاقة بين الدولتين. فقد وجّهت أمريكا أصابع الإتهام الى قراصنة صينيين ,بشأن الهجمات على مكتب ادارة شؤون الموظفين, وسرقة بيانات ٢٢ مليون شخص, والتي أدت الى تفاقم التوتر بينهما. فباكستان والهند, دولتان نوويتان, تقومان بالقرصنة المتبادلة, وفقا لباحثين في الأمن السيبراني. اما استونيا وبلاروسيا, فهما تتسابقان لبناء دروع دفاعية بوجه روسيا. وقد بدأ كلّ من الدنمارك ,ونزرلاند ببرامج لتطوير أسلحة سيبرانية هجومية , كما فعلت كلّ من الأرجنتين وفرنسا.[٣٥٠]

وفي بريطانيا, أعلنت الحكومة,عن نيّتها في زيادة الميزانية المخصّصة للحرب السيبرانية, عشرة أضعاف, لمواجهة تهديدات القرصنة الآتين من روسيا والصين. وكانت قيادة القوات المشتركة البريطانية, قد أعلنت عن توظيف ٣٠٠ اختصاصي في الميدان السيبراني, وعن تطوير مزيد من البرمجيات الخبيثة,

[350] http://www.cyberwar.news/2015-10-16-cyberwar-said-to-be-the-new-arms-race-as-nation-states-scramble-to-boost-capabilities-and-defenses.html

عدائية كانت أم تدخلية ,كالفيروسات, وأحصنة طروادة, والديدان, وبرامج التجسس, مما يتيح لأنظمة التكنولوجيا العسكرية, شل اتصالات العدو, أوعمليات قرصنة البنى التحتية. وكان ***بيتر روبرتز Peter Roberts*** , وهو مسؤول سابق في قيادة القوات المشتركة, وخبير في الحرب السيبرانية, قد صرّح أن "لبريطانيا شهية في أن تصبح لاعباً من الطراز العالي في الهجوم السيبراني". وأعلن ***فيليب هاموند Philip Hammond*** , أن بريطانيا تستطيع " الردع عندما تمتلك قدرات هجومية, سنبني في بريطانيا قدرة لتسديد ضربات سيبرانية, تمكننا من الرد في الفضاء السيبراني على من يهاجمنا."[٣٥١] وستستثمر الحكومة البريطانية, ١.٩ مليار استرليني, خلال السنوات الخمس القادمة, لحماية البلاد من الهجمات السيبرانية, وتطوير قدراتها السيادية في مجالها الإلكتروني تضمن لها, وفقا ل***هاموند*** "خطوات أكبر للدفاع عن نفسها, في الفضاء السيبراني, وبالمقابل, التمكّن من الرد, عند تعرّضها للهجوم."[٣٥٢]

ويقول ***هيبونن Hyppönen*** , وهو رئيس مكتب الأبحاث في الشركة الأهم عالميا , والمتخصّصة في الأمن السيبراني في هيلسنكي, ***F_Secure***: "لقد غيّرت رأيي بشأن الحرب السيبرانية, كنت أكره العبارة, وكنت أوضح للناس, في كلّ مرّة يسمعون أو يقرأون افتتاحيات عنها, بأن يعلموا أنها ليست حربا_ إنما هي تجسّس. حتى لو كانت الدول هي التي تقوم بها, فهي ليست حرب." ويتابع مستشهدا بالهجوم السيبراني الروسي على اوكرانيا, "عندما تكون دولتان في حالة حرب, وتستهدف البنى التحتية الحساسة, ليس بهدف السرقة, بل لقطع الكهرباء عن ٢٠٠ ألف شخص, فهذا ليس عملاً تجسسياً, إنما هو حرب سيبرانية. نحن في بداية سباق تسلح جديد, حيث السلاح أرخص, وأكثر فعالية, وأدق في تحديد الهدف من الأسلحة التقليدية, إضافة الى أنه يمكن إنكاره."[٣٥٣]

---

[351] Britain to start Pounds 2bn cyberspace offensive [Ulster Region] **Kerbaj, Richard; Shipman, Tim. Sunday Times** [London (UK)] 16 Aug 2015: 12. http://search.proquest.com.ezproxy.aub.edu.lb/docview/1704214792?pq-origsite=summon#

[352] **Britain's cyber security bolstered by world-class strategy** https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy

[353] Murdock,J.(2016),**Inside the new era of warfare: Exploring the 'cyber arms race' with Mikko Hyppönen**, http://www.ibtimes.co.uk/inside-new-era-warfare-exploring-cyber-arms-race-mikko-hypponen-1555084

ويقول **بيتر سنغر Peter Singer** , مدير مركز الأمن والاستخبارات, للقرن الحادي والعشرين في مركز ***بروكينغز Brookings,*** إنّ "هناك أكثر من مئة دولة تبني وحدات عسكرية سيبرانية , عشرون منها لاعبون أساسيون, وعدد صغير منها يمكنه تنفيذ حملة لحرب سيبرانية بأكملها. والخوف من أن تنتقل عدوى التسلّح السيبراني, الى باقي الدول. فنحن نشهد مظاهر سباق التسلح التقليدي نفسها, التي شهدناها إبان الحرب الباردة, أو قبل الحرب العالمية الأولى. فجوهر سباق التسلح, هو إنفاق الدول أكثر وأكثر, على بناء وتعزيز قدراتها العسكرية, لكن بإحساس أقل بالآمان, وهذا ما يميّز الفضاء السيبراني اليوم".[٣٥٤]

ويعتبر ***توماس ريد***, "أن الكثير من الدول تشعر اليوم, أنها بحاجة الى فصيلة سيبرانية, ايضا, لكي تؤخذ على محمل الجد. فما نراه اليوم, هو تصعيد في التحضير, فالدول تتحضر من خلال التكثيف الاستخباراتي, لأنها بحاجة للاستخبارات لتطور ادوات هجومية , كأنظمة مسح الضوئي لنقاط الضعف, او تكوين نظرة من الداخل حول كيفية عمل الاشياء, اي البحث عما يمكن عمله."

فالدول تبني جيشا رقميا وتحتاج الى تسليح هذا الجيش أي تطوير أنواع جديدة من الأسلحة. والدول الراعية للحرب السيبرانية, قد تستخدم بعضا من الأدوات التقليدية, كالقراصنة المجرمين, وهجوم تعطيل الخدمة, ولكن قد تلجأ الى ما هو أكثر تعقيدا, كستاكسنت مثلا. وهناك فارق كبير بين أسلحة سيبرانية عسكرية, وبين أدوات القرصنة, فالأولى أكثر تعقيدا ودمارا, وهي أكثر كلفة, وسريعة العطب وموجّهة أكثر نحو البرامج الصناعية, التي تدير خطوط الإنتاج, أو محطّات توليد كهرباء, أو شبكات الطاقة, كأنظمة سكادا SCADA,مثلا, هذه الأنظمة مفعّلة عبر شبكة الإنترنت, مما يجعلها عرضة للهجوم السيبراني.

لقد اتهمت الولايات المتحدة الاميركية مراراً الصين, باختراق شبكاتها الإلكترونية, واعتبرتها وروسيا, خطراً الكترونياً على أمنها. وتتهمها ايضاً باختراق نظم المعلومات العائدة للأقمار الصناعية التابعة لوكالة الفضاء الخارجي, ***ناسا***, الأمر الذي تنفيه الصين. وبالمقابل توجّه ايران وروسيا, الاتهام نفسه للولايات المتحدة الأمريكية. وتعدّ كلّ من السويد, وفنلندا, واسرائيل, من أفضل الدول التي لديها جهوزية لمواجهة الهجمات الالكترونية, مقارنة بالولايات المتحدة, والمانيا, وبريطانيا . ودفع عجز حلف الناتو في مواجهة

---

[354] Ranger,S. Inside the secret digital arms race: Facing the threat of a global cyberwar
http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/

الهجمات الالكترونية على استونيا وجورجيا, الى تكوين مركز للدفاع الالكتروني مقره تالين عاصمة استونيا. كما عمل الحلف على تطوير استراتيجيته, بحيث أصبح الفضاء السيبراني منطقة علمليات, وبات لزاما تطوير قدراته الدفاعية الالكترونية, بما يشمل مساندة ودعم حلفائه, الذين يتعرّضون لهجمات الكترونية, وأنّه وفقا لذلك, فإنّ أيّ هجوم يتم على أوروبا, أو أمريكا الشمالية, يعتبر هجوما ضد الجميع. وقام عدد من الدول, بتشكيل وحدات للحرب السيبرانية, ضمن قواتها المسلحة, كما شرعت الولايات المتحدة بتشكيل قيادة عسكرية للفضاء السيبراني, فيما اتجهت دول أخرى الى تخصيص ميزانيات للدفاع والأمن الالكتروني. هذا وتجري الولايات المتحدة سنويا تمارين, هي بمثابة محاكاة لحرب سيبرانية.

المبحث الثاني: تعاون دوليّ غير مقونن

يحظى الأمن السيبراني, اليوم, باهتمامٍ عالمي ملحوظ, جعل الدول تضعه في أولوية أجندتها. وبرز هذا الاهتمام, من خلال تزايد الاتفاقات السيبرانية الثنائية, في الآونة الأخيرة, بين الدول الرائدة اقتصاديا, بما فيها الاتحاد الأوروبي, والصين, والهند, وروسيا, والمانيا, وكندا, والولايات المتحدة الأميركية. اضافة الى تزايد المبادرات التعددية: كسعي دول مجموعة العشرين G20 الى الاتفاق على الاّ تسعى أيّة دولة من دولها, الى دعم أو القيام بعمليات سرقة للملكية الفكرية.أضف الى ذلك جهود دول منظمة شنغهاي للتعاون, الساعية الى إرساء اتفاق دولي, لإدارة الأمن المعلوماتي العالمي, ووضع جملة من المعايير, لبناء الثقة فيما بينها, في الفضاء السيبراني. كذلك اتخذت دول منظمة آسيان, ومنظمة الدول الأميركية, مبادرات مماثلة. كما تسعى الأمم المتحدة, الى ايلاء الصراع السيبراني اهتماما ملحوظا, من خلال عقد المؤتمر العالمي حول الفضاء السيبراني. إنّ تفاعل الناتو مع الهجمات السيبرانية على استونيا, برز جليا من خلال عقد اجتماع طارئ لمجلس شمالي الأطلسي, في عام ٢٠٠٧, تلتها قمّة بوخارست في عام ٢٠٠٨, حيث أعلن التحالف, عن أول سياسة له في الدفاع السيراني, واعتبر هذا الأمر, أول مناسبة تعلن فيه منظمة عسكرية عالمية, الزامية الدفاع الجماعي للأمن السيبراني, ومن خلال التأكيد على حق الدول الأعضاء في الرد, في حال تعرّض إحداها لهجوم سيبراني كارثي, وذلك تبعا للوسائل الواردة في السياسة التي وضعها, لتحقيق الأمن السيبراني.[٣٥٥] كما أن القطاع الخاص قام بخطوات لوضع أسس للتوصل الى فضاء سيبراني آمن, كمبادرة شركة مايكروسوفت, ودليل تالين.

المطلب الأول: تحقيق الأمن في الفضاء السيبراني

اعتبر وزير الداخلية الالماني, ***هانس بيتر فردريك*** ***Hans-Peter Friedrich*** , أنّ " السؤال الرئيسي للقرن الواحد والعشرين, هو كيفية تحقيق الأمن في الفضاء السيبراني". وشدّد على ضرورة ايجاد تفاهم عالمي, حول قواعد السلوك في هذا الفضاء. فعلى كلّ من الحكومات,ومصنّعي التكنولوجيا, ومستخدميها,

---

355 Hughes, R. (2008). NATO and global cyber defense'. In *The Bucharest Conference Papers, German Marshall Fund & Chatham House* (pp. 51-2).

تحمّل مسؤولية الآمان في شبكات الانترنت. ومن الضروري خلق وعي بمدى خطورة التهديد الذي تفرضه الجريمة السيبرانية, على هؤلاء الثلاث. [٣٥٦]

وأكّد ***كيث الكسندر***, على أهمية التعاون بين الحكومات وعالم الأعمال, قائلاً إنّ:" الشراكة هي جزء من الحلّ", وأنّ آليات الدفاع الفاعلة, في وجه التهديدات التي مصدرها الفضاء السيبراني, يمكن تحقيقها فقط من خلال التعاون والشراكة. كما أشار الى الحالة الطارئة للموضوع, قائلا إنّه" لا بدّ من فعل شيء اليوم". وحثّ نائب وزير الخارجية الاميركي لشؤون الأمن الداخلي, ***جين لوت Jane Holl Lute ,*** على استخدام كلّ الخيارات التقنية المتاحة, لحماية الفضاء السيبراني, معتبراً أنّ لا قدرة لأيّ حكومة, أن تحقّق منفردة الأمن السيبراني. أما ***نيللي كورس Neelie Kroes ,*** نائبة رئيس المفوضية الأوروبية, ومفوّض الإتحاد الأوروبي للأجندة الرقمية, قد توافقا على أنّ مرونة النظم, يمكن تحقيقها من خلال تعاون كل اللاعبين, على مختلف المستويات, مشيرين الى أن الهدف الرئيسي, هو إيجاد فضاء سيبراني آمن, قائلين " لا نريد سباق تسلح في الفضاء السيبراني". [٣٥٧]

وكما يشير دليل ***الناتو,*** حول وضع إطار للأمن السيبراني, الى اتفاق على أن الأعمال السيبرانية, هي أنشطة عسكرية شرعية, لكن لا يوجد توافق عالميّ, على القواعد التي يجب أن تطبق عليها."[٣٥٨]

وتجادل ***شكري,*** أن" الفضاء السيبراني يطرح مواضيع عالمية تحتاج للمعالجة, كما أنّه أوجد مجموعات جديدة, بمتطلبات جديدة , وميول جديدة, نحو الصراع والتعاون معا",[٣٥٩],كما تعتبر أنّ التعاون العالمي في هذا المجال, يرتكز على الاجابة على أسئلة ثلاثة: لماذا التعاون؟ ومتى التعاون؟ وكيف التعاون؟. فالدول تتعاون, إما لتحقيق اهداف لا تستطيع الوصول اليها بمفردها, وإمّا لأنذ الدول تواجه ظروفا معاكسة, تتطلب التنسيق, من أجل معالجة أكثر فاعلية. ومع اختلاف المصالح التي قد تؤدي الى التنافر

---

[356] Hegenbart,C. "We Do Not Want an Arms Race in Cyberspace." Hampton Roads International Security Quarterly. Transatlantic Euro-American Multimedia, LLC. 2013. Retrieved October,29,2016) from HighBeam Research: https://www.highbeam.com/doc/1P2-34521364.html

[357] Ibid,p:40

[358] Klimburg, A. (2013). National cyber security framework manual.,p:18 ,https://ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf

[359] Choucri, N. (2012). *Cyberpolitics in international relations*. MIT Press. P:156

بين الدول, يبقى العامل الاساسي هو مدى استعدادها للإنخراط في العمل الدولي المشترك, عبر التنسيق أو التعاون فيما بينها, للوصول الى اتفاق على كيفية العمل, لأنّ التعاون يفرض قيوداً على سيادة الدول, محلياً وخارجياً.

وترى شكري, أنّ المأسسة عالميا, تجري من أجل:

- وضع معايير وقواعد جديدة.
- الضغط على الدول التي تقاوم هذه المعايير , ودفعها الى الانصياع نحو الفهم الجماعي.
- التقليل من التشكيك, في العمليات والنتائج والمعلومات.
- خلق طرق مشتركة للاتصال والتفاهم.
- تسهيل الوساطة بين الاطراف المتنازعة, وتعزيز آفاق معالجة المشاكل.[٣٦٠]

وجاء في مؤتمر لمنظمة التعاون والنمو الاقتصادي, أنّه: " يجب على الانترنت, أن تمنح الشعوب الحق في التعبير عن طموحاتها الديمقراطية, على أن تعزّز السياسات المرتبطة بذلك الانفتاح, وأن ترتكز على احترام حقوق الانسان وسيادة القانون".[٣٦١] وهذا يعني ضرورة إخضاع الفضاء السيبراني, الى حد ما, للحوكمة. والاسئلة التي تطرح هنا, الى أي مدى يمكن أن يذهب هذا التنظيم؟ وأيهما أنسب الالزام ام التوافق؟ وأي سلطة لها الحق بذلك في التنظيم والمحاسبة؟ ولكن الحوكمة تفترض, كحدّ أدنى, التوصّل الى وضع معايير تقنية من قبل هيئة من الخبراء, توصّل المجتمع الدولي الى إطار قانوني شامل وملزم لتنظيم الفضاء السيبراني, كحدّ أقصى.

إنّ الأدوات المستخدمة لتحقيق الأمن السيبراني, ومواجهة الهجمات السيبرانية,اليوم, فاعلة ولكنها غير كافية لصدّها, نظرا لتطوّر الأنظمة السيبرانية و التي أصبحت أكثر تعقيدا, من جهة, وعدم القدرة على منع الهجمات السيبرانية المتطوّرة التي ترعاها الدول, بالتقنيات الدفاعية المتوافرة اليوم, من جهة ثانية.

---

[360] Ibid.p:157

[361] OECD High Level Meeting on the Internet Economy, ‘Communiqué on Principles for Internet Policy-Making’, 28–29 June 2011, p. 2, www.oecd.org/internet/innovation/48289796.pdf.

من هنا, يتوجّب على الدول, التفاوض حول اتفاقات دولية, شبيهة بتلك المتعلّقة بالأسلحة الكيميائية أو البيولوجية, تنصّ على كيفية إستخدام الأسلحة السيبرانية, و مشروعية استخدامها عند الرد على الهجوم, أو كيفية التعاطي مع المواطن القرصان في دولة ما, حتى يتم على أساسها توجيه الإتهام اليهما.

وترى د. ***منى الاشقر جبور***, أنّ "تراكم العناصر التي تجعل الفضاء السيبراني مجالا خطرا, يجعل السيطرة على ما يحدث فيه صعبة المنال, وغير فاعلة, منها على سبيل المثال, الامتداد العالمي للشبكة, وعدم وجود توافق دولي على القواعد الواجبة التطبيق, على سلوك الدول في هذا المجال, وسهولة ارتكاب الاعتداءات, ونتائجها الكارثية, كانتشار الفيروسات, واصابة الأنظمة غير المعنية وغير المستهدفة بالهجوم, يضاف الى ذلك المجهولية, التي تساعد الجهة المعندية, أو تساعد في تعقيد عملية الوصول اليها, أو حتى يمكنها أن تؤدي الى نسب الإعتداء الى جهة غير الجهة المعتدية, هذا دون أن ننسى الثغرات المعلوماتية في العديد من البرمجيات المستخدمة. وتشكل تقنيات المعلومات والاتصالات, مصدرا مقلقا للمخاطر, لا يمكن مواجهته خارج اطار التعاون الدولي"[٣٦٢]. وهذا ما أكّده الأمين العام للأمم المتحدة,بقوله:" إن جعل الفضاء السيراني مستقرا, وآمنا, لا يمكن الوصول اليه الاّ من خلال التعاون الدولي, على أن يكون القانون الدولي, وميثاق الأمم المتحدة, هما الأساس لهذا التعاون."[٣٦٣]

المطلب الثاني: القانونُ الدوليّ: مواكبةٌ ناقصة

إنّ القانون الدولي الحالي الذي ينظّم الأمور المتعلقة بالصراعات المسلحة (الدولية والغير دولية) لا يتضمّن عبارة الفضاء السيبراني. كما لا يتضمّن, أي قرار يتعلّق بالتغيرات الهائلة التي أحدثها هذا الفضاء, في السنوات العشرين الماضية في المجال الأمني. وهذا ما دفع بعض الدول الى إعادة تفسير القوانين الحالية, أو اتخاذ المبادرة بناء على قاعدة الضرورة, التي لا تعترف بالقانون. في الحالتين, قد تتهم الدول بخرقها للقانون الدولي, عندما يتعلّق الأمر باستخدام القوّة كطريقة لممارسة النزاع المسلح.

[362] الأشقر, السيبرانية هاجس العصر, ص:٩٩-١٠٠

[363] 70/174. Thirteenth United Nations Congress on Crime Prevention and Criminal Justice The General Assembly https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/443/27/PDF/N1544327.pdf?OpenElement

ويقول قاضي مشاة البحرية الأمريكي ***فيدا انتولين Vita Antolin*** , إنّ" أغلب الهجمات السيبرانية تقوم على عمليات, لا تلتقي والمعايير, التي يهدف القانون الدولي الى تنظيمها".[٣٦٤]

فالقانون الدولي, عاجز عن الإحاطة بالقضايا المتعلّقة بنشاطات الفضاء السيبراني, وذلك لأنّه وضع في النصف الأوّل من القرن العشرين, وكان هدفه حماية حقوق الإنسان وحماية ضحايا النزاعات المسلحة. فعلى سبيل المثال, في ظل القانون الحالي, في المادة ٥١ من ميثاق الأمم المتحدة, يجوز للدولة أن تتصرّف بصورة شرعية للدفاع عن نفسها عندما تواجه هجوما مسلحا. أما في سياق الحرب السيبرانية, تطرح هذه المسألة المزيد من التساؤلات بشأن متى يمكن اعتبار هجوم سيبراني معادلا لهجوم مسلح, ومن ثمّ ما إذا كان من الممكن أن يعزى الهجوم الى دولة ما. ويبدو أنّ "مسؤولية الدولة", تسلّط الضوء على التساؤل الأخير, فهي تنطوي على اقتراح أن كل دولة يتعيّن عليها أن تتصرّف, بحيث تمنع استعمال أراضيها لشن هجوم على دول أخرى, وإذا رفضت اتخاذ إجراءات وقائية, يمكن أن تعزى مسؤولية هذه الهجمات اليها. ولكن معظم الهجمات ليس لها مصدر جغرافي, كالبرمجيات الروبوتية الخبيثة, التي يمكن أن تنتشر عبر حدود متعددة, وتصدر من تحالفات تقع ضمن ولايات قضائية متعددة, أو ينفّذها وكيل يعمل بالنيابة عن مرتكبها الحقيقي. وفي بعض الأحيان, تكون الدولة نفسها عاجزة عن كشف الأطراف التي تتصرّف داخل أراضيها, أو التحقّق منها. وحتى إذا تمكّنت من تحديد هوية الطرف الذي يتصرف داخل منطقتها الجغرافية, فإن طبيعة الفضاء السيبراني تجعل من المستحيل لكيان واحد التحكّم على نحو شامل بهذا الصدد. وهكذا فإن الغموض لا يقتصر على مسألة المصدر فقط, بل يشمل مسألة التحكم ايضا.[٣٦٥]

المطلب الثالث: الحاجة الى اتفاقيةٍ دولية

لقد اقترحت كل من الصين, وروسيا, وطاجاكستان, واوزبكستان, مدوّنة لقواعد سلوك عالمية لأمن المعلومات, في دورة انعقاد الجمعية العمومية للأمم المتحدة ال٦٦. وكان يفترض بهذه الوثيقة, أن

[364] Antolin-Jenkins, V. M. (2005). Defining the parameters of cyberwar operations: looking for law in all the wrong places. *Naval L. Rev.*, *51*, p.134.

[365] حمدون توريه, السلام السيبراني.الاتحاد الدولي للاتصالات , ص:١٠٤-١٠٥

تشكّل انطلاقة لمناقشات على نطاق واسع لتنظيم السلوك السيبراني. لكن يبدو أن دولا أخرى, كالولايات المتحدة الامريكية, وعدد من الدول الأوروبية, تعارض فكرة الحاجة الى وضع مدوّنة لقواعد السلوك السيبراني, أو معاهدة تتعلّق بالحرب السيبرانية. بل أن هذه الدول ترى في هذه الالتزامات, تناقضاً مع القانون الدولي الحالي, القائم على مفاهيم ,مثل الإمتناع عن التهديد بالقوّة, (البند ٢ من المادة ٤ لميثاق الامم المتحدة) ,وحق الدفاع عن النفس عند حصول هجوم مسلح (المادة٥١ من ميثاق الأمم المتحدة) . وعلاوة على ذلك, فإنه من غير الواضح كيف أن مفاهيم وردت في المدوّنة المقترحة ك" الأنشطة العدائية" و" تهديد السلم والأمن الدولي", لها علاقة بالتهديد, أو استخدام القوّة, الواردة في ميثاق الأمم المتحدة., أو اذا ما كانت المدوّنة المقترحة تقيد الحق الأصيل في الدفاع عن النفس المنصوص عليه في المادة ٥١ من الميثاق. وهناك دول أخرى, تأخذ زمام المبادرة, لدفع النقاش والقرار, نحو ما تفرضه العواقب الإقتصادية والأمنية والوطنية, لما هو على المحك. وهذه الجهود أصبحت اكثر جديّة مع استخدام الستاكسنت. فمثلا, استضافت المملكة المتحدة, مؤتمراً حول قواعد السلوك في لندن عام ٢٠١١, للمساهمة في تأسيس حوار دولي حول الأمن السيبراني.[٣٦٦]

وكان الرئيس ***أوباما*** قد أشار إلى أنّ : "هدف الولايات المتحدة, ليس تكرار السباق في مجال التصعيد، مثل الذي رأيناه في الماضي في سباق التسلّح, وإنّما تحقيق اعتماد قواعد السلوك المسؤول في الفضاء الإلكتروني". ويذكر أنّ اعتماد فكرة قواعد سلوك للدول في الفضاء الإلكتروني، صدرت للمرة الأولى عن روسيا. ففي خريف عام ٢٠١١، بدأ الدبلوماسيون الروس, العمل على اتفاقية في الأمم المتحدة "لضمان أمن المعلومات الدولي"، تحدّد قواعد استخدام الإنترنت، مع الأخذ بعين الاعتبار, التحديات العسكرية, والسياسية, والجنائية, والإرهابية, بالإضافة إلى حظر استخدام الشبكة, للتدخّل في شؤون الدول الأخرى، وإسقاط الأنظمة غير المرغوب فيها. وعرضت روسيا, منح هذه الحكومة حرية واسعة للعمل ضمن "القطاعات الوطنية" للإنترنت. وناقشت الورقة أيضا, حظر عسكرة الفضاء الإلكتروني، وعلى وجه الخصوص، تجنب "استخدام تكنولوجيا المعلومات لأعمال عدائية"، بما في ذلك هجمات القراصنة. إلا أن المبادرة الروسية لم تحرز تقدما. واعتبرت الولايات المتحدة وحلفاؤها أنها تجسد رغبة الطرف الأضعف, للحد من إمكانيات الدول القوية, لتطوير تكنولوجياتها. ووصفت واشنطن إقتراح حظر البلدان تطوير تكنولوجياتها الهجومية بالأمر "غير الواقعي"، مشيرة إلى أن الترتيبات التقليدية (مثل معاهدة عدم انتشار

366 National Cyber Security Framework Manual,p:19,

الأسلحة النووية), لن تكون فاعلة في الفضاء الإلكتروني. واعتبرت طلب اعتماد مبدأ عدم التدخل في الشؤون الداخلية للدول, على شبكة الانترنت, ومنح الحكومات مزيدا من السلطة – "عنصر تحكّم لتعزيز رقابة الدولة على الشبكة"، في حين أن حكومة الولايات المتحدة، من حيث المبدأ، لا تعتبر أنه من الضروري اتخاذ أية قواعد خاصة لسلوك الدول في الفضاء السيبراني، على افتراض أن جميع القضايا العالقة, يمكن حلّها عبر المعايير الدولية القائمة. ويؤخذ على هذه القواعد, أنّها غير ملزمة ومع ذلك استغرق أمر الموافقة عليها عدة سنوات. والتكهّن بالموعد الذي ستصبح فيه هذه النوايا الحسنة قانونا، أمّر صعب للغاية اليوم، لا يتحمّل مسؤوليته حتى أكثر المتفائلين. وبسبب خصوصية التقنيات السيبرانية، من غير الواضح تماما كيفية مراقبة استخدام هذا القطاع, في غياب أيّة قيود. ومع الأخذ بعين الاعتبار، انعدام ثقة اللاعبين الرئيسيين ببعضهم البعض، سيستمر الجميع في تسليح أنفسهم.

إنّ هذا الوضع خطير أيضا, لأنّ الدول الرائدة في المجال المعلوماتي والإلكتروني، بما في ذلك روسيا والولايات المتحدة، وضعت الهجمات الإلكترونية, على قدم المساواة مع العمل العسكري التقليدي، معلنة عن حقها في الرد عليها, كعمل من أعمال العدوان. وبما أن تتبع مصدر الهجوم في الفضاء الإلكتروني صعب جدا، لا يمكن استبعاد أن أي طرف ثالث, سيحاول دفع موسكو وواشنطن إلى المواجهة.

ويبقى الأمل الوحيد معلقا على الخط الساخن، الذي أطلقه بوتين وأوباما في حزيران عام ٢٠١٣, بين موسكو وواشنطن, لمنع وقوع الحوادث السيبرانية, وتحولّها إلى أزمة شاملة. لذلك تأسّس خط تواصل معلوماتي يعمل على مدار الساعة. وهذا الخط, يماثل ذلك الذي أطلق في الحقبة السوفيتية, للحد من المخاطر في المجال النووي[٣٦٧]

المطلب الرابع: الاتفاقيةُ الأوروبيةُ... اتفاقيةٌ يتيمة

هل يمكن الاستعانة باتفاقية مجلس أوروبا لمكافحة الجرائم السيبرانية, والتي أقرّها مجلس أوروبا في عام ٢٠٠١، والتي تحبّذ الولايات المتحدة السير على نهجها, من أجل إبرام اتفاقية دولية في الفضاء السيبراني, نظرا لما طرحته هذه الاتفاقية من مسائل هامة, تتعلق بتنظيم استخدام الهجمات السيبرانية على

---

[367] الفضاء السيبراني..ساحة حرب جديدة قد تشعل العالم http://katehon.com/ar/article/lfd-lsybrny-sh-hrb-jdyd-qd-tshl-llm

صعيد النزاعات المسلحة؟ فوفقا لكل **من *ميشيل فاتس وستبتو جونسون*** ***Michael A. Vatis and Steptoe E. Johnson***, [٣٦٨]

هناك ثلاث مسائل تطرحها هذه الاتفاقية:

أولاً: نطاق الهجمات الإجرامية السيبراني

ألزمت الإتفاقية الدول الأطراف, بأن تصدر التشريعات القانونية المحلية, التي تجرّم سلوكيات محدّدة (الدخول الى كامل أو جزء من منظومة الكمبيوتر, وإعتراض إرسال البينات ,الى, أو من, أو خلال منظومة كمبيوتر, واتلاف, أو محو, أو إفساد, أو تعديل, أو تدمير بيانات موجودة على الكمبيوتر, وإعاقة عمل المنظومة, عن طريق إدخال, أو إرسال, أو إتلاف, أو محو بيانات الكمبيوتر...) [٣٦٩]

ثانياً: إجراءات التحقيق

عالجت الاتفاقية طرائق إثبات وقوع الجريمة, وتحديد هوية مرتكبها في مواد عدة. فتحديد المكان ,والزمان, وهويّة مرتكب الجريمة السيبرانية, هو مفتاح لتحريك المسؤولية الدولية.[٣٧٠]حيث تبدأ إجراءات التحقيق, من تتبّع سير البيانات المخزّنة والتحفّظ عليها, من أجل تمكّن السلطات المختصّة, القيام بمهامها التحقيقية, والكشف عن المنفّذين_ لأن أخطر ما في أمر تحريك المسؤولية الجنائية, هو تمكّن مرتكبيها من إخفاء البيانات, أو تدميرها بعد تنفيذ الهجوم_ الى آلية التعامل مع أي شخص, بحوزته الكمبيوتر الذي استخدمت في تنفيذه الجريمة, وإلزام مقدّم خدمة الإنترنت في إقليم دولة طرف, توفير التسهيلات اللازمة, والمعلومات المتعلّقة بالمشترك بالخدمة (المتهم), وصولا الى الولاية القضائية, والقانون المطبّق على المتهمين بارتكاب هذه الجرائم[٣٧١]

---

[368] National Research Council, (. (U.S.), & National Academies, (. (U.S.). (2010). *Proceedings of a Workshop on Deterring Cyberattacks : Informing Strategies and Developing Options for U.S. Policy*. Washington, D.C.: National Academies Press ,p: 207-2018

[369] Convention on Cybercrime, Budapest, 23.XI.2001, articles 2,3,4,5 http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[370] الفتلاوي, أحمد, الهجمات السيبرانية : مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر ٢٠١٥-٢٠١٦, وزارة التعليم العالي والبحث العلمي,جامعة الكوفة,كلية القانون,ص:٣٥

[371] Convention on Cybercrime, articles 14,16,17,18,22

ثالثاً: تعيين نظام سريع وفاعل للتعاون الدولي

نصّت المادة ٢٣ من الاتفاقية, على تعاون الدول الأطراف لأقصى درجة ممكنة, لأغراض التحقيق, أو جمع الأدلّة الخاصة بالجريمة الجنائية الإلكترونية ." كما نصت المادتان ٢٤ و ٣٥ من الاتفاقية, على تسليم المجرمين. وإنشاء وسيلة للتواصل تدعى بشبكة ٧/٢٤ ,لضمان توافر المساعدة الفورية, لأغراض التحقيقات أو جمع الأدلة المتعلقة بهذه الجرائم.[٣٧٢]

وعلى الرغم من كون الاتفاقية وسيلة فاعلة لمكافحة الجرائم السيبرانية, الا أنها لاقت معارضة من منظمات حقوق الانسان الأوروبية, كونها ستمنح الحكومات حق مراقبة الأفراد, في الفضاء السيبراني. كما امتنعت روسيا, وهي عضو في مجلس أوروبا, عن التوقيع على الاتفاقية, والبعض يعزو السبب الى رغبتها في تجنّب الالتزامات, التي تفرض عليها تقديم مساعدات للدول الأخرى وتتعلّق باجراءات التحقيق حول الجرائم الالكترونية, نظراً لكون العديد منها منبثق منها أو برعايتها.[٣٧٣]

وعلى عكس أميركا, فإنّ روسيا لا ترى إمكانية الاعتماد على هذه الاتفاقية, لتنظيم الهجمات السيبرانية, بل لا بد من إبرام اتفاقية دولية معنية بالهجمات السيبرانية, تأخذ بعين الاعتبار القواعد الدولية الخاصة بالحد من التسلّح, كما اقترحت عنوانا لها : الاتفاقية الدولية المعنية بالحد من الأسلحة السيبرانية.[٣٧٤]

وقد لاقت الاتفاقية تأييدا واسع النطاق من جهات متعددة, كمنظمة التعاون لآسيا والمحيط الهادئ, والإنتربول, ومنظّمة الدول الأميركية والقطاع الخاص. كما اعتبرها, كلّ من ***فاتس وجونسون*** , الأكثر واقعية في مكافحة الجريمة السيبراينة, والأكثر قبولاً من أطراف دولية متعددة في الوقت الراهن .

رغم مصادقة الولايات المتحدة الاميركية, والكثير من الدول الأوروبية عليها, عانت هذه الاتفاقية من القصور, إن لجهة عدم تصديق لاعبين رئيسيين في الفضاء السيبراني عليها, كالصين وروسيا, و الدول الآسيوية, والأفريقية , ودول أميركا الجنوبية, أو لجهة نصّها على امكانية تمنّع الفرقاء في الاتفاقية, عن تقديم المساعدة, عند تعارض ذلك مع قوانينها المحلية, أو عند إعلانها أن في ذلك مسّا بسيادتها الوطنية, أو نظامها الداخلي. كذلك لجهة عدم وجود آلية تلزم الدول بتطبيق الاتفاقية, او لجهة الغموض

---

[372] *Informing Strategies And Developing Options For U.S. Policy* .p:207-217

[373] Ibid,p:218

[374] فتلاوي, الهجمات السيبرانية ,ص: ٣٧

الذي اعترى الكثير من التعريفات, المتعلقة بالجرائم والهجمات السيبرانية, ما يجعلها عرضة لاساءة الفهم أو التأويل, أو تفسيرها تبعاً لمصالح الدول.[٣٧٥]

المطلب الخامس: ثنائية التعاون

في ٢٧ نيسان ٢٠١٦, استضافت روسيا المنتدى الصيني- الروسي للأمن السيبراني, والذي انتهى باتفاق البلدين على متابعة هدف واحد وهو"السيادة المستقلة لكل دولة في الفضاء السيبراني". لكن هذا الهدف يتناقض مع المفاهيم الغربية, لا سيّما الولايات المتحدة الاميركية, التي تدعو الى فضاء سيبراني مجاني, ومتاح للجميع متخطّيا حدود الدولة الجغرافية, ومبدأ سيادتها. وكانت الولايات المتحدة الاميركية والصين, توصّلتا الى اتفاق ثنائي في عام ٢٠١٥, حول التجسس في الفضاء السيبراني, رغم اختلاف مقاربتي كلّ من الدولتين في هذا الفضاء. وقد تضمّن هذا الإتفاق, أربع مبادرات رئيسية:

- عدم قيام أحد البلدين بدعم, أو القيام مباشرة, بنشاطات سيبرانية تتعلّق بسرقة الملكية الفكرية, كالأسرار التجارية, والمعلومات المتعلّقة بالشركات الخاصة, والقطاعات التجارية.
- التعاون بين البلدين في تقديم المعلومات المتعلقة بالأنشطة الالكترونية الخبيثة, التي تجري داخل أراضيها, أو المناطق الخاضعة لولايتها.
- وضع إطار بيروقراطي لإجراء حوار سيبراني, على مستوى عال.
- مشاركة البلدين في تطوير القواعد التنظيمية لأنشطة الدولة, في الفضاء السيبراني.[٣٧٦]

والإتفاق الصيني- الأمريكي في الميدان السيبراني, ليس ملزماً للدولتين, ولا يعدو كونه عبارة عن ضبط للنفس, وذلك حماية لاقتصاد البلدين.ففي تقرير صادر عن مركز الدراسات الاستراتيجية الدولية, لعام

---

375 *Informing Strategies And Developing Options For U.S. Policy* ,p:220

376 FACT SHEET: President Xi Jinping's State Visit to the United States, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

٢٠١٤, تراوحت التكلفة العالمية للجرائم السيبرانية, وجرائم التجسس بين ٣٧٥ بيليون دولار و٥٧٥ تريليون دولار سنويا.[377]

أما التعاون السيبراني الروسي – الصيني, فيركّز أكثر على العنصر الحضاري في الفضاء السيبراني, إضافة الى أمن البيانات, والقضايا الاجتماعية على الشبكة الالكترونية, لا سيما التطرّف الديني. والجدير بالذكر, أن كلّ من الصين وروسيا, تواجهان المشاكل نفسها التي يواجهها الغرب في الفضاء السيبراني, لكن الفارق هو الرقابة التي تفرضها كل منهما على استخدامات المواطنين لهذا الفضاء. والأهم من ذلك, التشديد على أهمية حق الدولة في السيادة في الفضاء السيبراني, وبالتالي الحق في فرض قيودها عليه, وهذا ما أكدته الدولتان في منتدى الأمن السيبراني لعام ٢٠١٦. وهذه ليست المرة الأولى التي تشدّد فيه روسيا والصين على أهمية الحفاظ على سيادة الدول في الفضاء السيبراني, فقد سبق المنتدى, توقيع اتفاق حول الأمن السيبراني, في أيار ٢٠١٥, تضمّن بالاضافة الى تعهّد هما بعدم القيام بهجمات سيبرانية, وبتبادل المعلومات والتقنيات بين الأجهزة المسؤولة عن تطبيق القوانين في البلدين, وتنسيق المواقف الدولية, التأكيد على مبدأ سيادة الدولة في الفضاء السيبراني.[378] فهل هناك من تناقض بين التعاون السيبراني الصيني – الروسي, والتعاون السيبراني الصيني– الأمريكي؟ في الواقع, إنّ الجميع متفقون على أهمية التعاون بين هذه الدول, لتحقيق الأمن السيبراني, عند الضرورة, ولكن الإتفاق الصيني – الأمريكي, ينحو أكثر نحو تأمين الحماية الاقتصادية في الفضاء السيبراني, في حين أن الإتفاق الصيني– الروسي, يميل أكثر نحو تنظيم قضايا ذات طابع اجتماعي. فليس هناك من صدام بين الأهداف الاقتصادية والاجتماعية للعلاقة بين الدوليتين السيبرانيتين. كما أنه من الناحية الدبلوماسية, لم تنكر الاتفاقية الصينية – الأميركية, صراحة عمليات التجسس السياسية, التي قد تقوم بها إحدى الدولتين. كذلك فإن الصين وروسيا, لم تدخلا الأمن السيبراني, في استراتيجية الأمن القومي لبلديهما.

---

377 "Net Losses: Estimating the Global Costs of Cybercrime" (Center for Strategic and International Studies, June 2014) http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

378 **China and Russia Support "Cyber Sovereignty"** http://chinadigitaltimes.net/2015/05/china-and-russia-agree-to-respect-cyber-sovereignty/

إنّ مسؤولية الدولة الرئيسية, تكمن في حماية البيانات الشخصية لمواطنيها, كون هذه البيانات, لها علاقة بضمان الرفاهية, والاستقرار المادي لكل فرد. بمعنى آخر, إنّ الاتفاقات بين الدول الثلاث, الولايات المتحدة الأميركية, وروسيا, والصين, وضعت الأسس الأمنية للسكان بشكل عام. وتستدعي مسؤولية الدول في الحفاظ على أمنها القومي, من التهديدات الخارجية القيام بالتجسّس السيبراني, واستخدام أساليب الرقابة على الحكومات, ووكالات الاستخبارات, التابعة للدول الأخرى. ومن هنا, فليس لهذه الدول الثلاث, أيّة مصلحة في وضع قيود على استخدام التجسّس السيبراني بحق الدول الأخرى. ما يعني صعوبة التوصّل الى اتفاقية, تنظّم قواعد السلوك في الفضاء السيبراني.[٣٧٩]

المطلب الخامس: جهود مجموعة العشرين

أما عن جهود مجموعة العشرين G20, وتحديدا في القمة التي عقدت في تركيا في عام ٢٠١٥, فلقد صدر عن القادة المجتمعين, والذين يمثلون أكبر الدول الاقتصادية في العالم, بيان هام يتعلّق بالأمن والاستقرار الدولي في الفضاء السيبراني,جاء فيه:

- التأكيد على أن القانون الدولي, بما فيه ميثاق الأمم المتحدة, ينطبق على سلوك الدول في الفضاء السيبراني. مما يعني وفقا لهذه الدول, أنّ هذا الفضاء ليس ب"الغرب البري"" Wild West ", وبالتالي لا قانون له, بل هو مكان حيث سلوك الدول تحكمها القواعد المطبقة في الميادين الأخرى. مع العلم أنّ هذا القانون بحاجة للكثير للاحاطة بالمخاطر الجديدة, فرضها الميدان السيبراني.
- أكد قادة مجموعة العشرين, بمن فيهم قادة كل من البرازيل والصين والهند وروسيا, على المعيار المطروح من الولايات المتحدة الأمريكية, أنّه لا يحق لأية دولة, القيام من خلال الفضاء السيبراني, بسرقة الملكية الفكرية, أو دعم من يقوم بها. ومنها الأسرار التجارية, والمعلومات التجارية السرية, لصالح شركات او قطاعات تجارية مناقسة.[٣٨٠]

---

379 Comparing Cyber-Relations: Russia, China, and the U.S.
http://mackenzieinstitute.com/comparing-cyber-relations-russia-china-and-the-u-s/

380 Painter,Ch.(2011),G20: Growing International Consensus on Stability in Cyberspace,
https://blogs.state.gov/stories/2015/12/03/g20-growing-international-consensus-stability-cyberspace

المطلب السابع: للقطاع الخاص دور: مبادرات اللاعبين من غير الدول

إن المعادلة التي تقوم عليها مسألة تنظيم الفضاء السيبراني, تحتاج الى تضافر جهود الدول والمنظمات الدولية الحكومية, كالأمم المتحدة, والإتحاد الأوروبي, والمنظمات الدولية غير الحكومية, كاللجنة الدولية للصليب الأحمر. بالمقابل سجّلت مبادرات من قبل كيانات, ليست دولا لتنظيم الفضاء السيبراني, منها:

فقرة أولى: شركة مايكروسوفت :المبادئ الدولية للأمن السيبراني

أطلقت شركة مايكروسوفت مبادرة تحت عنوان:" تقليص النزاع في عالم معتمد على الانترنت", وذلك في كانون الأول من عام ٢٠١٤. [٣٨١] لكنها لم تكن المبادرة الأولى للقطاع الخاص من هذا النوع. فقبل خمس عشرة عاما, حثّ ***ستيف كايس Steve Case***, الدول على أن تراجع قوانينها المركزية, وأن تتبنّى المعايير الدولية للحوكمة في إدارة عالم الإنترنت, بما فيها الحماية, والخصوصية, والضريبة[٣٨٢]. ولكن مبادرة مايكروسوفت, هي أول نص شامل لمعايير محددة حول السلوك على شبكة الإنترنت , وعلى رغم كونها مبادرة مصدرها القطاع الخاص, الاّ أنها تضمّنت معايير لتنظيم سلوك الدول. كما هدفت بشكل أساسيّ, الى الحد من اساءة استخدام تكنولوجيا المعلومات, او استغلال الدولة لها من خلال اعتبارها جزءا من العمليات العسكرية. كما نصّت المبادرة, على ست مبادئ للأمن السيبراني, دعت من خلالها الدول الى تحسين دفاعاتها السيبرانية, والحد من انخراطها في عمليات هجومية.[٣٨٣]

فقرة ثانية: دليل تالين

في عام ٢٠١٣, نشرت مجموعة من الخبراء, وعلى رأسهم البروفسير ميشال شميت Schmitt Michael دليل تالين حول القانون الدولي المنطبق على الحرب السيبرانية ,تحت رعاية استونيا . فقد قام هؤلاء, بدراسة تبعات الحرب السيبرانية والقانون المنطبق عليها, واعتبروا أنّ اللجؤ الى العمليات في الفضاء السيبراني, أثناء النزاعات المسلحة , قد يكون له تبعات إنسانية وخيمة. ورأى الخبراء, أنّه لا بد من التأكيد

---

[381] McKay, A., Neutze, J., Nicholas, P. ,Sullivan, K.(2014), International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World,Microsoft http://aka.ms/cybernorms

[382] Goldsmith, J., & Wu, T. (2006). *Who controls the Internet?: illusions of a borderless world*. Oxford University Press.

[383] McKay et al (n 60) 2

على الصلة بين القانون الدولي الانساني, والتكنولوجيا الجديدة, عند استخدامها أثناء النزاعات المسلحة. فوسائل الحرب تتطوّر مع مرور الوقت, ومن الواضح أنّه لم تعد مثلما كانت عليه عند صياغة اتفاقيات جنيف عام ١٩٤٩, وبالتالي هناك حاجة الى تطوير القانون لضمان الحماية للمدنيين في الفضاء السيبراني, وعلى الدول أن تقرر هذا الأمر بنفسها. ويوضح الدليل, أنّه نتاج لآراء للخبراء أنفسهم, وليس للدول أو المنظّمات التي ينتمون اليها.[٣٨٤] وكما يبدو من العنوان, يحافظ الدليل على نموذج عسكري واضح, مع التركيز على قانون الحرب (jus ad bellum), وقانون الصراع المسلح (jus in bello). ويحدّد النص خمسة وتسعين قاعدة, تم تبنيها بالإجماع, من مجموعة الخبراء المندفعين, نحو استنساخ القانون الدولي العرفي. [٣٨٥]

وقد وجّهت إنتقادات عدّة لدليل تالين, منها تركيزه , بشكل أساسي, على النشاطات السيبرانية التي تحدث فوق مستوى استخدام القوة ,حيث أنّ معظم, إن لم تكن كلّ العمليات السيبرانية, تصنّف تحت هذه العتبة.[٣٨٦] لكن هذه القواعد التي نصّ عليها الدليل, هي أكثر تحديدا ودقة من مبادئ الأمن السيبراني, التي وضعتها مايكروسوفت. فمثلا, القاعدة رقم ٣٧, تنص على حظر الهجوم السيبراني بحق أهداف مدنية, في سياق الصراع المسلح.[٣٨٧] فالعبارتان الأساسيتان, الهجوم السيبراني والأهداف المدنية, حدّدتا بدقة في الدليل.[٣٨٨] رغم بعض الخلاف حول تطبيق القاعدة في ظروف معينة, يبقى المضمون واضحاً, ومحدّدا بشكلٍ كاف, ومؤسسا لانطلاقة لمنظومة حقوق وواجبات, في الفضاء السيبراني. كما تختلف المبادرتان من نواح هامة, فالمبادئ التي قدّمتها شركة مايكروسوفت, هي اقتراحات واسعة فقط, بمعنى أنه يقع عاتق الدول تحويلها الى التزامات محددة.[٣٨٩]

لكن ما يتشارك فيه كل من المبادرة أو الدليل, هو كونهما صادرين عن جهات غير حكومية, وبالتالي لا صفة الزامية لهما. فشركة مايكروسوفت, أشارت الى أن عملها كان محفّزا للدول, كي تضع المعايير

[384] Tallinn Manual 111

[385] Ibid, 6

[386] Fleck, D. (2013). Searching for international rules applicable to cyber warfare—A critical first assessment of the new Tallinn manual. *Journal of Conflict and Security Law*, *18*(2),331-351.

[387] Tallinn Manual (n 39) 124.

[388] Ibid, 91 (definition of cyber attack) and 125 [3] (definition of civilian objects)

[389] McKay et al (n 60) 12.

المقترحة على المسار الذي يجعلها سياسيا وقانونيا ملزمة.[٣٩٠] كذلك أشار دليل تالين في افتتاحيته, الى كونه "وثيقة غير ملزمة",[٣٩١] ففي مجال الأمن الجماعي, تبقى الدول هي المشرّع الاساسي, في النظام القانوني الدولي.[٣٩٢]

هناك فضاء سيبراني واحد, يتشاركه كلّ من الجيش والمستخدمين المدنيين, حيث كل ما فيه متشابك ومترابط. وتتمثل التحديات في توخي الحذر من الحاق الضرر بالمدنيين, وبالبنى التحتية المدنية وضمان توجيه الهجمات السيبرانية ضد الأهداف العسكرية فقط. فالقانون الدولي الانساني, لا ينظّم العمليات السيبرانية التي تقع خارج سياق النزاع المسلح. ومن القضايا الرئيسية, ضرورة تحديد الظروف, التي يمكن في إطارها اعتبار العمليات السيبرانية, تحدث في سياق نزاع مسلح, أو تكون في حد ذاتها سببا في اندلاع نزاع مسلح, بحيث ينطبق عليها القانون الدولي الانساني.

لكنّ الأمم المتحدة تحثّ الدول على المضي قدما, نحو بدء مفاوضات دولية, من خلال سلسلة من القرارات التي صدرت عنها, لكن دون أن تجد لها صدى في المحافل الدولية .[٣٩٣] وكل المبادرات الدولية المعنية بتنظيم استخدام التكنولوجيا لأغراض عسكرية, ما زالت في إطار النقاش الحذر, وتخضع الى الموازنة بين المصالح القومية للدول, وحقها بالدفاع عن نفسها, وبين الآثار الغير إنسانية, التي قد تتسبّب بها.

390 Ibid, (n 60) 3.

391 Tallinn Manual(n 39) 1

392 Mačák, K. (2016, May). Is the international law of cyber security in crisis?. In *Cyber Conflict (CyCon), 2016 8th International Conference on* (pp. 127-139). IEEE.

393 الفتلاوي, الهجمات السيبرانية,ص:٣٩

الخاتمة

إنّنا أمام فضاء جديد, بكل ما للكلمة من معنى, فرض وقائع جديدة, وحتّم مراجعة بعض النظريات, كما أعاد قولبة مفاهيم عدّة, كالقوة والسلام والحرب...

وإذا كان من الممكن, تلمّس معالمه, فإنّه من الصعب, الإحاطة بها بصورة واقعية, وذلك لاعتبارات عدّة. ويزيد من الصعوبة, تسارع التحوّلات فيه, بشكل يعجز الباحث أحيانا, عن مجاراتها, وتصبح وتيرة المعالجات, آنيّة, قصيرة الأمد, وربما عديمة الصلاحية.

لكن العزم على مقاربته, وسبر أغواره, يجب أن يتوطد ويتعزّز, نظرا لما يطرحه من تحدّيات استثنائية, تطاول تقريبا, أوجه الحياة كافة, للأفراد والجماعات والدول.

لقد حاولت في رسالة بحثي, هذه إبراز أهمية القوة السيبرانية, كقوة جديدة أفرزها الفضاء السيبراني, نظرا للمزايا التي تتمتع بها, في ظل تنافس الدول على امتلاكها, وسعيها لتوظيفها في مجالات جدّ حيوية. وفي ظل الغموض التي يشوب استخدامها, وعدم القدرة على التحكّم بفاعليها, وتعدّد اللاعبين الذين يقبضون على أزمّتها, سادت المخاوف من انزلاقات لا تحمد عقباها, لا سيّما لجهة تأزيم العلاقات بين الدول. يعزّز تلك الخشّية, بروز مصطلحات, وملاحظة نشاط محموم تحت عناوين لافتة: عسكرة الفضاء السيبراني, سباق التسلّح السيبراني, الحرب الالكترونية, وبرل هاربور سيبرانية.

على إنّ ذهاب بعض الاكاديميين, الى اعتبار أنّ اندلاع حرب سيبرانية, أمرٌ مبالغ فيه, لا يجعل من غير الواقعي أيضاً, النظر الى الفضاء السيبراني, كساحة حرب, يستخدم فيها سلاح المعلومات, وحيث تشنّ عمليات سيبرانية, إمّا بشكل مستقلّ, وإمّا لمواكبة صراع مسلّح.

لقد أضحى الأمن السيبراني, من أولى أولويات الدول, تبتكر باسمه النظريات وترسم استراتيجيات, وترصد له موازنات ضخمة. وحيث أن مخاطر انتهاكه تتجاوز الحدود, وتهدّد سيادة الدول, فإنّه من الطبيعي, والحالة تلك, أن يصبح هماً دولياً, وأن يطرح بإلحاح مسألة تعاون الدول, على صيانته, وترسيخه. ذلك أنّ الفضاء السيبراني, هو في نهاية المطاف, من صنع الإنسان, فهو الذي يبنيه ويمتلكه. ولطالما فرضت التفاعلات بين البشر, ايجاد حوكمة لتنظيمها. والأنشطة السيبرانية, لا سيما المرتكزة على علاقات القوة, ليست مستثناة من هذه القاعدة.

وتبقى أهم محدّدات المواجهة القانونية, متمثّلة في ما يأتي:

- تحديد المقصود من استخدام القوة في الفضاء السيبراني.
- تحديد مدى اعتبار الهجوم الكتروني هجوما مسلحا, وبالتالي طبيعة الأساليب المستخدمة, ومستويات الاستجابة المتناسبة مع الهجمات السيبرانية.
- كيفية تحديد المسؤولية القانونية, والجهات الفاعلة المشاركة في العمليات السيبرانية, ومدى امكانية تحقيق التوازن بين متطلّبات الأمن القومي, وصون حماية الحرية الفردية للمواطنين, والاستخدام السلمي للفضاء السيبراني.
- مدى استجابة الدول للكشف عن قدراتها الالكترونية من الأسلحة, والتي تعتمد بالأساس على الإبتكار, والبحث والتطوير, والسريّة.
- عشوائية مناطق الاستهداف, واطلاق الهجمات السيبرانية عبر الحدود الدولية بما قد يتسبب بالضرر لطرف ثالث, ويخل بأمن الفضاء السيبراني, بشكل عام.
- امكانية استخدام الأسلحة السيبرانية, من قبل جماعات إرهابية, ما يتطلّب من الدول والمنظّمات الدولية أن تتحرّك لمكافحة التهديدات التي يمثلها هذا التطوّر, واتخاذ مجموعة من الاجراءات, التي من شأنها الحد من انتشار الأسلحة السيبرانية. كالقرار الصادر عن مجلس الأمن الدولي, رقم ١٥٤٠, عام ٢٠٠٤ , والذي عمل على الحد من انتشار الأسلحة الكيماوية, والبيولوجية, والنووية.

وعليه, يقع على عاتق المجتمع الدولي بالدرجة الأولى, قوننة الأعمال الحربية أو العدائية, في ما يسمّى الساحة الخامسة للمعركة. وهنا, أطرح عدة تساؤلات:

- هل إنّ العمل المؤسساتي الدولي هو السبيل التنظيمي الناجح للحوكمة, وذلك من خلال خلق منظّمة سيبرانية دولية, ذات آلية مراقبة ومحاسبة فاعلة, تتمكّن الدول فيها من وضع قواعد تنظيمية ملزمة للأمن السيبراني؟ وفي حال تمّ انشاء مثل هذه المنظمة, هل تكون العضوية فيها حكرا على الدول, أم يستدعي الأمر ضرورة إشراك أصحاب القرار من غير الدول, نظرا لما لهؤلاء من دور فاعل في هذا الفضاء؟ وكيف نجعل هذه المنظّمة بعيدة عن هيمنة الدول الكبرى؟
- هل يشكّل التوافق على الصعيد الاقليمي, انطلاقة نحو اتفاقية سيبرانية شاملة؟ فلقد سعت بعض الدول, الى تنظيم استخدام تكنولوجيا المعلومات, في ظل اتفاقيات إقليمية, حدّدت الإطار القانوني للسلوك الإجرامي, والعقوبات الواجب ايقاعها على كل من يستخدم تكنولوجيا المعلومات, لأجل

الحصول على منافع مادية أو معنوية أو بهدف زعزعة أمن المجتمع, واستقراره, وبمختلف جوانبه الاقتصادية والصحية ووحدته.[٣٩٤] ويصحّ القول, إنّ هذه الاتفاقيات, قد تكون حجر أساس لإبرام اتفاقيات دولية, لا لأجل تنظيم استخدام تكنولوجيا المعلومات, في النطاق الداخلي للدولة الطرف في الاتفاقية, فحسب, بل أيضا من أجل كبح جماح استخدامها, بهدف تهديد السلم والأمن الدوليين.

- هل تستطيع المناقشات الثنائية الحالية أن تسهم في تحقيق الاستقرار في الفضاء السيبراني, وبالتالي السلم والأمن الدوليين؟
- هل يجب خصخصة الأمن السيبراني, حيث إنّ القطاع الخاص يعمل بسرعة أكبر, وبأقل بيروقراطية من الحكومات, وذلك عبر شراكة مع القطاع العام, يسمح فيه هذا الأخير لشركات الحماية الالكترونية في المساهمة في تطوير معايير الدولة التقنية, والإطّلاع الدوري على قدرات الدولة الدفاعية السيبرانية.
- هل يمكن للمبادرات الخاصة, والاقليمية, والعالمية أن تتكامل فيما بينها لايجاد توافق دولي للحوكمة السيبرانية, وبالتالي إمكانية وضع اتفاقية سيبرانية دولية؟ هل يمكن لهذه الاتفاقية أن تمنع وقوع هجمات افتراضية يكون لها التأثير الذي كان ليبرل هاربور, أو هيروشيما, أو أحداث ١١/٩؟ هل يمكن للاتفاقية أن تتماشى مع السرعة الهائلة التي تشهدها تكنولوجيا المعلومات, أم أنّها ستصبح عديمة الصلاحية قبل أن يجفّ حبرها؟

وقد يتساءل البعض, لماذا لم يتوصّل المجتمع الدولي بعد الى عقد اتفاقية دولية, لحظر استخدام الهجمات السيبرانية, أو لوضع ضوابط قانونية لاستخدامها على الأقل؟ هل المصالح الدولية تقف عائقا أمام هكذا اتفاقيات, لا سيما مصالح الدول التي تحتكر أو تهيمن على قطاع البرامج الإلكترونية للاغراض العسكرية؟

---

[394] ورد في الفقرة الثالثة من ديباجة الاتفاقية المتعلقة بالجريمة السيبرانية ما نصه:" واقتناعا بضرورة الحاجة الى اتباع سياسة جنائية مشتركة– كمسألة أولوية – تهدف الى حماية المجتمع ضد الجريمة الالكترونية, وذلك من خلال عدة أمور منها إقرار التشريع الملائم ودعم التعاون الدولي", أنظر : مجلس اوروبا,"اتفاقية مجلس اوروبا المتعلق بالجريمة الالكترونية"

ويقول ***سكوت شاكيلوفرد Scott Shackelford*** "، أنّ الاختلاف في وجهات النظر حول حظر تكنولوجيا المعلومات في النزاعات المسلحة, هو ذاته القائم بين الدول الحائزة للأسلحة النووية, إذ لا يزال الغموض يكتنف موقف المجتمع الدولي من حظرها, على مستوى اتفاقية متعددة الأطراف".[٣٩٥]

كما أنّ التحدّي الأكبر للتنظيم, هو عدم وجود إرادة دولية للقيام بالمفاوضات, أو لإصدار التشريعات القانونية الملزمة, يقابل ذلك كما رأينا سابقا, تسارع في التسلّح السيبراني. لقد أدّى هذا التحدّي الى إثارة نوع من الضبابية, حول قدرة أو عدم قدرة القانون الدولي العام والانساني, على كبح آثار الهجمات السيبيبرانية, لا سيّما أنّ القانون الدولي الإنساني, يذهب الى تنظيم استخدام الأسلحة, في حين لا يبدو أنّ الهجمات السيبرانية تصنّف على هذا النحو. ويذهب قاضي مشاة البحرية الاميركية ***فيدا انتولين*** الى القول:" أن اغلب الهجمات السيبرانية, تقوم على عمليات, لا تلتقي والمعايير التي يهدف القانون الدولي الى تنظيمها."[٣٩٦]

ومن التحدّيات كذلك, استخدام تكنولوجيا المعلومات من لاعبين من غير الدول. إذ غالبا ما تعلن تلك المجموعات, مسؤوليتها عن هجمات سيبرانية ألحقت أضرارا جسيمة في قطاعي الاتصالات والاقتصاد, فضلا عن مخاطرها الانسانية الأخرى . لكن ذلك لا يقف حائلا دون إبرام اتفاقية دولية, تحظّر تصرّفات معينة, سواء ارتكبت من قبل دول أو من غير الدول.

وقد يكون السبب في تأخر إبرام معظم الاتفاقيات, ذات الصلة بوسائل وطرائق القتال, عدم رغبة الدول المتقدمة في الصناعة العسكرية, في الدخول في اتفاقيات دولية, قد تحظر عليها وسائل تساعد في حفظ أمنها, تحت مسميات الضرورة العسكرية. هذا الأمر, دفع بالأمم المتحدة وبعض الدول الى الإعلان صراحة,عن النيّة بدعم أي توجّه دوليّ يفضي الى حظر, أو تقييد استعمال أنظمة الكترونية, معدّة للاستخدام العسكري أو الأمني وفقا لما استقرّ عليه القانون الدولي العام المقنّن فضلا عن العرف الدولي, والسوابق القضائية, وآراء كبار فقهاء القانون. وكان ***بان كيمون Ban Ki-moon*** , الأمين العام للأمم

---

395 S. J. Shackelford & R. B. Andres, (2010).State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. *Geo. J. Int'l L.*, *42*, 971.

396 Antolin-Jenkins, V. M. (2005). Defining the parameters of cyberwar operations: looking for law in all the wrong places. *Naval L. Rev.*, *51*, p:134

المتحدة (٢٠٠٧-٢٠١٦), أول مسؤول أمميّ يدعو لإبرام اتفاقية دولية متعددة الاطراف, تنظّم مسألة الهجمات السيبرانية. [٣٩٧]

ولكن الصعوبة التي ترافق تحديد مسؤولية المهاجم السيبراني, قد تجد لها حلا, فيما لو أبرمت اتفاقية دولية تحدّد صور إسهام الدول في الهجمات السيبرانية (دون حصرها في نقاط معينة نظرا للتطور الدائم الذي يشهده الفضاء السيبراني), كتحديد نقطة انطلاق البيانات, اضافة الى نوع هذه الهجمات, وآثارها, أثناء الهجوم أو بعده.

فهل ترجح الكفّة نحو التعاون المتعدّد الأطراف(Multilateral) ليكون الخيار الأفضل لتنظيم الفضاء السيبراني, بعيدا عن المأسسة أو الخصخصة, وذلك من خلال وضع اتفاقية أو وثيقة, هل ستذهب الاتفاقية المتعددة الاطراف, نحو الحظر أم التقييد؟ وهل ستتعهّد الدول الأطراف بعدم دعم المجموعات من غير الدول, وعدم توظيفها لخدمة مصالحها.

من الواضح, أن الاجابة المفصّلة والدقيقة, تستلزم معالجات, تتخطّى حدود رسالتنا, يبقى أنّا مقتنعون, أنّ الاتفاقات المتعدّدة الأطراف, من شأنها أن تؤمّن الاستقرار, وتقلّل من التصعيد, عبر التركيز على نواح محدّدة كبناء الثقاء بين الدول, لا سيّما تلك المتنافسة سيبرانيا, ووضع مقاييس للشفافية, وخلق قواعد خاصة بالمسؤولية عن سلوكياتها في الفضاء السيبراني, وتوسيع الفهم المشترك حول تطبيق القانون الدولي على الصراع السيبراني, وزيادة التطمين حول الحدّ من الهجمات السيبرانية.

اذا كانت القوننة إحدى سمات النظام الدولي اليوم, فإنّ الأمر نفسه يجب أن ينطبق على المجتمع الرقمي المتشابك عالميا". فقد تتعدّد أشكال الصراعات وتتنوّع استخدامات القوّة, الاّ أنّ المطلوب واحد: ضبطها والسيطرة عليها قدر الإمكان. وهذه برأينا, إحدى اسطع وابهى أمثولات التاريخ.

---

[397] فتلاوي, الهجمات السيبرانية, ص ٣٤

لائحة المراجــع

المراجع باللغة العربية:

المؤلفات:

١. الأشقر(منى جبور), السيبرانية هاجس العصر, الطبعة الأولى,المركز العربي للبحوث القانونية والقضائية,بيروت ٢٠١٦

٢. توريه. حمدون, السلام السيبراني. الاتحاد الدولي للاتصالات أحمد نصر زين. (٢٠١٥).

٣. الحراري (خالد), مفهوم القوة في السياسة الدولية , الطبعة الأولى, دار المستقبل, مطابع الأهرام, جمهورية مصر العربية ٢٠١٥

٤. رحومة (علي محمد),علم الاجتماع الآلي,مقاربة في علم الاجتماع العربي والاتصال عبر الحاسوب,سلسلة عالم المعرفة, المجلس الوطني للثقافة والفنون والآداب,الكويت ٢٠٠٨

٥. عبد الصادق(عادل),الإرهاب الإلكتروني القوة في العلاقات الدولية: نمط جديد وتحديات مختلفة,المركز العربي لأبحاث الفضاء الالكتروني,الطبعة الثانية,القاهرة,٢٠١٣

٦. عبد الصادق(عادل),الفضاء الالكتروني والعلاقات الدولي: دراسة في النظرية والتطبيق, الطبعة الأولى, المكتبة الأكاديمية,جمهورية مصر العربية,٢٠١٦

دراسات:

١. خليفة عبد العال (إيهاب عبد الحميد)، استخدام القوة الإلكترونية في إدارة التفاعلات الدولية: الولايات المتحدة الأمريكية نموذجا خلال الفترة من ٢٠٠١ إلى ٢٠١٢ The Journal of the Faculty of Economics . and Political Science, 16(2), 202-206.

٢. رجب (إيمان) ، "تأثير الهوية على سلوك الفاعلين من غير الدول فى المنطقة العربية: دراسة حالتى حزب الله وحركة حماس"، رسالة ماجستير (جامعة القاهرة، كلية الاقتصاد والعلوم السياسية، ٢٠١٤) تعلقيات مصرية ، مركز الاهرام للدرسات السياسية والاستراتيجية ، العدد١٣٠:١٢يوليو٢٠٠٩.

٣. عبد الحليم (فضل الله), علاقة المواطن بالسلطة في العصر الرقمي,المركز الاستشاري للدراسات والتوثيق,٢٠١٣

٤. عبد القادر (علي احمد), المنوفي كمال ,النظريات والنظم السياسية , الطبعة الاولى يناير ٢٠٠٢

٥. الفتلاوي(أحمد عبيس نعمة)الهجمات السيبرانية :مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم الدولي المعاصر ٢٠١٥-٢٠١٦, وزارة التعليم العالي والبحث العلمي,جامعة الكوفة,كلية القانون.

٦. يوسف فاروق, القوة السياسية, القاهرة ,مكتبة عين شمس ١٩٨٤

مجلات وصحف

١. **السَّايْبِر ساحة "خَفِيَّة" لحربٍ "ناعِمَة" قادِمة https://www.lebarmy.gov.lb/ar/content ! العدد ٨٩ - تموز ٢٠١٤**

٢. الفضاء السيبراني..ساحة حرب جديدة قد تشعل العالم http://katehon.com/ar/article/lfd-lsybrny-sh-hrb-jdyd-qd-tshl-llm

مواقع الكترونية

١. عبد الصادق عادل ،أمريكا وتشكيل قيادة عسكرية في الفضاء الإلكتروني. هل بدأ الاستعداد لحروب المستقبل؟ http://www.assakina.com/news/news1/9379.html

٢. قبل "ياهو": هذه أبرز عمليات القرصنة الإلكترونية http://www.akhbarlibya.net/arabic-news/216982.html

مراجع اللغة الإنكليزية:

المؤلفات:

1. Armitage, R. L., & Nye, J. S. (2007). *CSIS Commission on Smart Power: a smarter, more secure America*. CSIS.
2. Art R. A Grand Strategy For America [e-book]. Ithaca: Cornell University Press; 2003 p:. Available from: eBook Collection (EBSCOhost), Ipswich, MA. Accessed August 6, 2016.
3. Barlow, J. P. (1990). *Crime & Puzzlement* (pp. 44-48). Electronic Frontier Foundation.
4. Betz, D. J., & Stevens, T. (2011). Chapter One: Power and cyberspace. *Adelphi Series*, *51*(424), 37-38
5. CARAYANNIS, E., Campbell, D. F., & Efthymiopoulos, M. P. (2014). *Cyber-Development, Cyber-Democracy and Cyber-Defense* (pp. 279-301). Nueva York: Springer.
6. Choucri, N. (2012). *Cyberpolitics in international relations*. MIT Press.
7. Choucri, N., & Clark, D. (2011). Cyberspace and International Relations: Toward an Integrated System. *Explorations in Cyber International Relations Project*, 208-25.
8. Clarke, R. A., & Knake, R. K. (2011). *Cyber war*. HarperCollins.
9. Clough, J. (2015). *Principles of cybercrime*. Cambridge University Press.
10. Cornish, P., Livingstone, D., Clemente, D., & Yorke, C. (2010). *On Cyber Warfare*. Chatham House.
11. Coughlan, S. M. (2016). *Is There a Common Understanding of What Constitutes Cyber Warfare?*. Lulu Press, Inc.

12. Cross, Mai'a K. Davis, Europe as a Smart Power: The Impact of the European External Action Service (August 8, 2011). APSA 2011 Annual Meeting Paper. Available at SSRN: http://ssrn.com/abstract=1900094
13. Dahl, R. A. (2005). *Who governs?: Democracy and power in an American city*. Yale University Press.
14. Ducheine, P., & Van Haaster, J. (2014, June). Fighting power, targeting and cyber operations. In *Cyber Conflict (CyCon 2014), 2014 6th International Conference On* (pp. 303-327). IEEE.
15. Dyson, E. (1997). *Release 2.0: A design for living in the digital age*. Broadway Books.
16. Eriksson, J., & Giacomello, G . "The Information Revolution, Security, and International Relations": (IR) relevant theory? International Political Science Review Vol. 27, No. 3 (Jul., 2006), p . 231 http://www.jstor.org.ezproxy.aub.edu.lb/stable/pdf/20445053.pdf
17. Friedman, T. L. (2000). *The Lexus and the olive tree: Understanding globalization*. Macmillan.p:107
18. Gibson, W. (2000). *Neuromancer*. Penguin.
19. Goldsmith, Jack, and Wu, Tim. Who Controls the Internet : Illusions of a Borderless World. Cary, US: Oxford University Press (US), 2006 p147-161. ProQuest ebrary. Web. 9 October 2016.
20. Joint Chiefs of Staff, Joint Publication 1-02, Dictionary of Military and Associated Terms (JP 3-0), Department of Defense, Washington D.C., 8 November 2010 p:58
21. KAGAN, R., 2003, Paradise and Power ,America and Europe in the new world order p:27-29
22. Kramer, F. D., Starr, S. H., & Wentz, L. K. (2009). *Cyberpower and national security*. Potomac Books, Inc.
23. Krasner, S. D. (1999). *Sovereignty: organized hypocrisy*. Princeton University Press. P 11-25
http://site.ebrary.com.ezproxy.aub.edu.lb/lib/aub/reader.action?docID=10031906
24. Kuehl, D. T. (2009). From cyberspace to cyberpower: Defining the problem. *Cyberpower and national security*, 26-28.
25. Lewis, J. A., & Timlin, K. (2011). *Cybersecurity and cyberwarfare: Preliminary assessment of national doctrine and organization*. UNIDIR.
26. Mattern, J. B. (2005). WhySoft Power'Isn't So Soft: Representational Force and the Sociolinguistic Construction of Attraction in World Politics. *Millennium-Journal of International Studies*, *33*(3), 583-612.

27. Mearsheimer, J. J. (2001). *The tragedy of great power politics*. WW Norton & company.p:7https://samuelbhfauredotcom.files.wordpress.com/2015/10/s2-mearsheimer-2001.pdf
28. Mulvenon, J. C., & Rattray, G. J. (Eds.). (2012). *Addressing Cyber Instability: Executive Summary*. Cyber Conflict Studies Association.
29. Nye,Joseph S. 'Foreword', in Henry and Peartree (eds), The Information Revolution and International Security
30. Ottis, R., & Lorents, P. (2010, April). Cyberspace: Definition and implications. In International Conference on Information Warfare and Security (p. 267). Academic Conferences International Limited.
31. PUB, J. (1994). Department of Defense Dictionary of Military and Associated Terms.
32. Rattray, G. J. (2009). An environmental approach to understanding cyberpower. *Cyberpower and National Security*, 253-274.
33. Rifkin, J. (2011). *The third industrial revolution: how lateral power is transforming energy, the economy, and the world*. Macmillan.
34. Rowland, J., Rice, M., & Shenoi, S. (2014). The anatomy of a cyber power.*International Journal of Critical Infrastructure Protection*, *7*(1),p:4
35. Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.
36. Schreier, F. (2015). *On cyberwarfare*.
37. Toffler, A., & Toffler, H. (1995). *Creating a new civilization: The politics of the third wave*. Turner Pub.
38. Van Haaster, J. (2016, May). Assessing cyber power. In *Cyber Conflict (CyCon), 2016 8th International Conference on* (pp. 7-21). NATO CCD COE.
39. Waltz, K. (1979). Theory of international relations. *Reading: Addison-Wesley*.
40. Wiener, N. (1961). *Cybernetics or Control and Communication in the Animal and the Machine* (Vol. 25). MIT press.

دراسات:

1. "Net Losses: Estimating the Global Costs of Cybercrime" (Center for Strategic and International Studies, June 2014) http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf
2. Antolin-Jenkins, V. M. (2005). Defining the parameters of cyberwar operations: looking for law in all the wrong places. *Naval L. Rev.*, *51*, 132. Shackelford, S. J., & Andres, R. B. (2010).

3. Arquilla, J., & Ronfeldt, D. (1992). Cyberwar Is Coming', P-7795. *Santa Monica, CA: RAND*.
4. Bachrach, P., & Baratz, M. S. (1963). Decisions and nondecisions: An analytical framework. *American political science review*, *57*(03), 632-642.
5. Barlow, J. P. (1996). A cyberspace independence declaration. *URL:https://www.eff.org/cyberspace-independence*
6. Barnett, M., & Duvall, R. (2005). Power in international politics. *International organization*, *59*(01), 39-75. Retrieved from http://www.jstor.org/stable/3877878
7. Bieber, F. (2000). Cyberwar or sideshow? The Internet and the Balkan wars. *Current History*, *99*(635), 124.
8. Book review: "Cosmopolitan Power in International Relations" by Giulio M. Gallarotti 09 Aug. 2015 / Oliver Stuenkel
9. Brown, G. D. (2013). Fourteenth Annual Sommerfeld Lecture-The Wrong Questions about Cyberspace, The. *Mil. L. Rev.*, *217*, 214.
10. Carter, A. (2015). The DOD cyber strategy. *Department of Defense: Washington, DC*.
11. Cavelty, M. D., & Mauer, V. (2016). *Power and security in the information age: Investigating the role of the state in cyberspace*. Routledge.
12. Clarke, R. (2009). War from cyberspace. *The National Interest*,P:32 http://users.clas.ufl.edu/zselden/coursereading2011/Clarkecyber.pdf(last visited 19,10,2016)
13. Cooper, Hard power, soft power and the goals of diplomacy,p:167-180.
14. Dahl, R. A. (2005). *Who governs? Democracy and power in an American city*. Yale University Press.
15. Digeser, P. (1992). The Fourth Face of Power. *The Journal of Politics, 54*(4), 979. Retrieved from http://www.jstor.org/stable/2132105
16. Eric Talbot Jensen, Cyber Deterrence, 26 EMORY INT'L L. REV. 773, 785–86 (2012)
17. Fleck, D. (2013). Searching for international rules applicable to cyber warfare—A critical first assessment of the new Tallinn manual. *Journal of Conflict and Security Law*, *18*(2), 331-351.
18. Franzese, P. W. (2009). Sovereignty in Cyberspace: Can it exist. *AFL rev.*, *64*, 1.
19. GAILE-SARKANE, E., & ŠČEULOVS, D. Cyberspace vs. Electronic Environment: The Case of Europe.
20. Gartzke, E. (2013). The myth of cyberwar: bringing war in cyberspace back down to earth. *International Security*, *38*(2), 41-73.

21. GEORGE W. BUSH, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES 3 (2006),p:9 https://www.comw.org/qdr/fulltext/nss2006.pdf
22. Geun, L. (2009). A soft power approach to the "Korean wave". *The review of Korean studies*, *12*(2), 123-137.
23. GOURLEY, S. K. (2013). Cyber Sovereignty. *Conflict and Cooperation in Cyberspace: The Challenge to National Security*, 279-280
24. Gray, K. R., & Friedman, T. L. (2005). The World is Flat: A Brief History of the Twenty-First Century.
25. Hart, J. (1976). Three Approaches to the Measurement of Power in International Relations. International Organization, 30(2), 289-305. Retrieved from http://www.jstor.org/stable/2706260
26. Lewis, J. (2011). Cyberwar thresholds and effects. *IEEE Security & Privacy*, *9*(5), 23-29.
27. Luber, D. R., & Wilkinson, D. H. (2009). Defining Cyberspace for Military Operations. *Marine Corps Gazette*, *93*(2), 40.
28. McKay et al (n 60) 2. The complete list of the proposed norms may be found in the annex to the document: ibid 20
29. Menthe, D. C. (1997). Jurisdiction in cyberspace: a theory of international spaces. *Mich. Telecomm. & Tech. L. Rev.*, 70-71
30. National Research Council (, National Academies (. *Proceedings Of A Workshop On Deterring Cyberattacks : Informing Strategies And Developing Options For U.S. Policy* [e-book]. Washington, D.C.: National Academies Press; 2010. Available from: eBook Academic Collection (EBSCOhost), Ipswich, MA. Accessed November 13, 2016.p:218
31. Nye Jr, Joseph S. "The benefits of soft power." *Harvard Business School Working Knowledge* 2 (2004), http://hbswk.hbs.edu/archive/4290.html
32. Nye Jr, Joseph S. *Cyber power*. HARVARD UNIV CAMBRIDGE MA BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, 2010
33. Nye, J. (1990). The Changing Nature of World Power. Political Science Quarterly, 105(2), 177-192. doi:1. Retrieved from http://www.jstor.org/stable/2151022 doi:1
34. Nye, J. (2008). Public Diplomacy and Soft Power. The Annals of the American Academy of Political and Social Science, 616,p:99 . Retrieved from http://www.jstor.org/stable/25097996

35. Nye, J. S. (2002). Limits of American power. *Political Science Quarterly*, *117*(4), 545-559
36. Nye, J.S. Soft Power: The Means to Success in World Politics, (New York, Public Affairs Press, 2004) http://belfercenter.hks.harvard.edu/files/joe_nye_wielding_soft_power.pdf
37. Paganini, P. (2012). The Rise of Cyber Weapons and Relative Impact on Cyberspace. *Infosec Institute, Elmwood Park, Illinois(http://dx. doi. org/resources. infosecinstitute. com/the-rise-of-cyber-weapons-and-relative-impact-on-cyber space*.
38. Parker, K. L., & Force, U. A. (2014). The Utility of Cyberpower. *Military Review*, *94*(3), 26.
39. Pearlman, W., & Cunningham, K. G. (2012). Nonstate actors, fragmentation, and conflict processes. *Journal of Conflict Resolution*, *p:2 56*(1), 3-15. doi:10.1177/0022002711429669
40. Petallides, C. J. (2012). "Cyber Terrorism and IR Theory: Realism, Liberalism, and Constructivism in the New Security Threat." *Inquiries Journal/Student Pulse*, *4*(03). Retrieved from http://www.inquiriesjournal.com/a?id=627
41. Rattray, G. J., & Healey, J. (2011). Non-state actors and cyber conflict. *America's Cyber Future: Security and Prosperity in the Information Age*, *2*, 65-86.
42. Rattray, G., & Healey, J. (2010). Categorizing and understanding offensive cyber capabilities and their use. In *Proceedings of a Workshop on Deterring Cyberattacks, Informing Strategies and Developing Options for US Policy*(pp. 77-97).
43. Rex Hughes, 'NATO and global cyber defense', The Bucharest Conference Papers, German Marshall Fund & Chatham House, 2008, pp.51-2
44. Rifkin, J. (2000). The age of access: The new culture of hypercapitalism. *Where All of Life is a Paid-For Experience, Tarcher, New York*, *33*, 40-51.
45. Rowland, J., Rice, M., & Shenoi, S. (2014). The anatomy of a cyber power. *International Journal of Critical Infrastructure Protection*, *7*(1), 3-11.
46. Shackelford, S. J., & Andres, R. B. (2010). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. *Geo. J. Int'l L.*, *42*, 971.
47. Shen, Y. (2016). Cyber Sovereignty and the Governance of Global Cyberspace. *Chinese Political Science Review*, *1*(1), 81-93.
48. Smit, H. (1965). International Litigation Under the United States Code. *Columbia Law Review*, *65*(6), 1015-1046. https://www.law.cornell.edu/uscode/text/18/1030
49. Thomas Rid and Peter McBurney, "Cyber Weapons," Rusi Journal, February/ March 2012, https://www.rusi.org/downloads/assets/201202_Rid_and_ McBurney.pdf

50. Troxell, J. F. (2012). Military power and the use of force. *US Army War College Guide to National Security Strategy, 5th Ed., Carlisle, PA: Strategic Studies Institute, US Army War College*, 224-225.
51. Turner, M. (2014). Is There Such a Thing as a Violent Act in Cyberspace?. *International Security and Intelligence Summer School 2013, Pembroke College, and the University of Cambridge*.
52. U.S. DEP'T OF DEF., NATIONAL DEFENSE STRATEGY 16 (2008), available at http://www.defenselink.mil/news/2008/20national /20defense /20strategy.pdf.
53. Waltz, K. N. (2000). Structural realism after the Cold War. *International security*,p;14
54. Waterman, S. (2007). Who cyber smacked Estonia?
55. Wilhelmsen, V. C. R. (2014). SOFT WAR IN CYBERSPACE How Syrian non-state actors use hacking to influence the conflict s battle of narratives.
56. Wilson, C. (2008, January). Botnets, cybercrime, and cyberterrorism: Vulnerabilities and policy issues for congress. LIBRARY OF CONGRESS WASHINGTON DC CONGRESSIONAL RESEARCH SERVICE. https://www.fas.org/sgp/crs/terror/RL32114.pdf(last visited 13,10,2016)
57. Wilson, E. J. (2008). Hard power, soft power, smart power. *The Annals of the American Academy of Political and Social Science*, *616*(1), 110-124.

أطروحات:

1.Buijs,G. (2012). The Relative Power Of Bits and Bytes,Cybersecurity in power perspective

2.Pallaver, M. (2011). *Power and its forms: hard, soft, smart* (Doctoral dissertation, London School of Economics).

أفلام وثائقية :

1. "No Maps for These Territories". Docurama.com http://www.docurama.com/docurama/william-gibson-no-maps-for-these-territories/
2. Ralph Langer , “Destructive Cyber Weapons”(December 2011) https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon?language=en?utm_source=tedcomshare&utm_medium=referral&utm_campaign=tedspread

تقارير :

1. "We do not want an arms race in cyberspace,"Hegenbart, Christine.
2. "Desktop Search Engine Market Share", April2013 http://www.netmarketshare.com/search-engine-market share.aspx?qprid=4&qpcustomd= Kaspersky Lab,'Stuxnet Worm:Insight from Kaspersky Lab'http://www.kaspersky.com/au/about/news/virus/2010/Kaspersky_Lab_provides_its_insights_on_Stuxnet_worm
3. 70/174. Thirteenth United Nations Congress on Crime Prevention and Criminal Justice The General Assembly https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/443/27/PDF/N1544327.pdf?OpenElement
4. Assembly, UN General. 2010. Report of the group of Governmental experts on developments in the field of information and telecommunications in the context of international security. A/65/201. http:// www.unidir.org/pdf/activites/pdf5-act483.pdf. (last visit:10,11,2016)
5. Bilbao-Osorio, B., Dutta, S., & Lanvin, B. (2013, April). The global information technology report 2013. In *World Economic Forum* p74-60
6. Cyberattacks an 'existential threat' to U.S., FBI says,FBI official warns about increasing cyber-sophistication of rogue states, criminals http://www.computerworld.com/article/2516690/cybercrime-hacking/cyberattacks-an--existential-threat--to-u-s---fbi-says.html
7. DHS, 'National Strategy to Secure Cyberspace', viii and 6
8. Gavel, Doug. "Joseph Nye on Smart Power." *interview with Joseph S. Nye, Harvard Kennedy School Insight Interview* 3 (2008). http://belfercenter.ksg.harvard.edu/publication/18419/joseph_nye_on_smart_power.html **Hampton Roads International Security Quarterly** (Apr 1, 2013): 39.
9. House of Representatives, 'National Defense Authorization Act for Fiscal Year 2012', 629. http://www.rules.house.gov/Media/file/PDF_112_1/legislativetext/HR1540conf.pdf
10. Hundley, R. O., Anderson, R. H., Bikson, T. K., Dewar, J. A., & Green, J. (2000). *The Global Course of the Information Revolution: Political, Economic, and Social Consequences Proceedings of an International Conference*. RAND NATIONAL DEFENSE RESEARCH INST SANTA MONICA CA. http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf (last visited 16,10,2016)

11. Jensen, E. T. (2015). Cyber Sovereignty: The Way Ahead. *Tex. Int'l LJ*, *50*, 275.
12. Kirlin, J. P. (1926). REPORTS OF INTERNATIONAL ARBITRAL AWARDS RECUEIL DES SENTENCES ARBITRALES. *CONTRACT*, 162-163. http://legal.un.org/riaa/cases/vol_II/829-871.pdf (last visited 10,11,2016)
13. Liaropoulos, A. (2015). Exercising State Sovereignty in Cyberspace: An International Cyber--Order Under Construction?. *Leading Issues in Cyber Warfare and Security: Cyber Warfare and Security*, *2*, 191.
14. Mačák, K. (2016, May). Is the international law of cyber security in crisis?. In Cyber Conflict (CyCon), 2016 8th International Conference on (pp. 127-139). NATO CCD COE.
15. OECD High Level Meeting on the Internet Economy, 'Communiqué on Principles for Internet Policy-Making', 28–29 June 2011, p. 5, www.oecd.org/internet/innovation/48289796.pdf.
16. Report of the Working Group on Internet Governance Château de Bossey June 2005,p:5 http://www.wgig.org/docs/WGIGREPORT.pdf
17. *Sheldon, J. B. (2011). Deciphering cyberpower: Strategic purpose in peace and war. AIR UNIV MAXWELL AFB AL STRATEGIC STUDIES QUARTERLY.*
18. Van Haaster, J. (2016, May). Assessing cyber power. In Cyber Conflict (CyCon), 2016 8th International Conference on (pp. 7-21). NATO CCD COE.
19. Winner, J. L., Holt, L. S., Duran, J., & Watz, E. (2010). *Cyber Operations Virtual Environment*. LUMIR RESEARCH INST GRAYSLAKE IL.
20. World(Microsoft 2014) http://aka.ms/cybernorms

قرارات :

1. S.C. Res. 661, U.N. Doc. S/RES/0661 (Aug. 6, 1990)
2. S.C. Res. 674, U.N. Doc. S/RES/0674 (Oct. 29, 1990)
3. S.C. Res. 678, U.N. Doc. S/RES/0661 (Nov. 29, 1990)
4. S.C. Res. 1680, U.N. Doc. S/RES/1680 (May 17, 2006)
5. G.A. Res. 47/121, U.N. Doc. A/RES/47/121 (Dec. 18, 1992)
6. S.C. Res. 1234, U.N. Doc. S/RES/1234 (Apr. 9, 1999)

7. UN Security Council, Resolution 1113 (2011), 5 March 2011

8. Convention on Cybercrime, Budapest, 23.XI.2001, articles 2,3,4,5 http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

9. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

دوريات مجلات وصحف يومية:

1. "Don't mess with us," The Economist, January 2, 2010, 31
2. Lynn, W. J. (2011). The Pentagon's Cyberstrategy, One Year Later. *Foreign Affairs*, *28*.
3. https://www.foreignaffairs.com/articles/2011-09-28/pentagons-cyberstrategy-one-year-later
4. Soft Power and Smart Power in Africa by Maj. James R. "Hack" Hackbarth, USAF p:4 http://www.journal.forces.gc.ca/vo1/no3/doc/50-56-eng.pdf
5. Gallarotti, G. M. (2011). Soft Power: what it is, why it's important, and the conditions for its effective use. *Journal of Political Power*, *4*(1), 25-47.
6. Angela McKay et al, International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent
7. Britain to start Pounds 2bn cyberspace offensive [Ulster Region] **Kerbaj, Richard**; **Shipman, Tim**. **Sunday Times** [London (UK)] 16 Aug 2015: 12. http://search.proquest.com.ezproxy.aub.edu.lb/docview/1704214792?pq-origsite=summon#
8. Comparing Cyber-Relations: Russia, China, and the U.S.,http://mackenzieinstitute.com/comparing-cyber-relations-russia-china-and-the-u-s/
9. **Computer Spies Breach Fighter-Jet Project**,By **SIOBHAN GORMAN**, April 21, 2009 http://www.wsj.com/articles/SB124027491029837401 9.cwur.org/2016.php

10. **CYBER DEFENSE, DOD's $6.7B cyber budget focused on emerging threats**,BY KEVIN MCCANEY,FEB 10, 2016 https://defensesystems.com/articles/2016/02/10/dod-2017-cyber-budget.aspx

11. David Barrett, Internet Records to be Stored for a Year, TELEGRAPH, Apr. 5, 2009, http://www.telegraph.co.uk/technology/news/5105519/Internet-records-to-be-stored-for-a-year.html (last visited 16,10,2016)

12. David E. Sanger and Michael S. Schmidt, "More Sanctions on North Korea After Sony Case," New York Times, January 2, 2015 http://www.nytimes.com/2015/01/03/us/in-response-to-sony-attack-us-levies-sanctions-on-10-north-koreans.html

13. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," New York Times, June 1, 2012

14. Dod report on China details escalation in the cyber domain https://defensesystems.com/articles/2016/05/16/dod-report-china-cyber-domain.aspx

15. Electricity Grid in U.S. Penetrated By Spies ,By SIOBHAN GORMAN ,Updated April 8, 2009 http://www.wsj.com/articles/SB123914805204099085

16. Bumiller, E. and Shanker, T.(2012), "Panetta Warns of Dire Threat of Cyberattack," New York Times http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?_r=0 (last visited 13,10,2016)

17. Nakashima, E. & Warrick ,J.(2012), Stuxnet Was Work of U.S. and Israeli Experts, Officials Say, WASH. POST http://www.washingtonpost.com/world/national-security/stuxnet-was-work-ofus-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html

18. Nakashima,,E.(2015), "U.S. decides against publicly blaming China for data hack," Washington Post

19. Ex-NSA chief: Safeguards exist to protect Americans' privacy **By MIchael Hayden, CNN Contributor**

20. **China and Russia Support "Cyber Sovereignty" http://chinadigitaltimes.net/2015/05/china-and-russia-agree-to-respect-cyber-sovereignty/**

21. **China Blocks Access to Google's Gmail as Ban Escalates** https://www.bloomberg.com/news/articles/2014-12-29/china-blocks-access-to-google-s-gmail-as-ban-escalates

22. Forbes,"Shopping for zero-days,A price list for Hackers" secret software exploits"2012 http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/#3a29ac706033

23. Foreign Affairs, ‘Chinese Computer Games’, https://www.foreignaffairs.com/articles/china/2012-03-01/chinese-computer-games
24. Rashid,Y.F.(2012), “Coding Errors in Shamoon Malware Suggest It May Be the Work of Amateurs,” Security Week http://www.securityweek.com/coding-errors-shamoon-malware-suggest-it-may-be-work-amateurs
25. Ferguson, N. (2003). Power. *Foreign Policy*, *134*, 18-24.
26. http://edition.cnn.com/2013/08/01/opinion/hayden-nsa-surveillance/
27. Haass, R. N. (2008). The age of nonpolarity: what will follow US dominance.*Foreign Affairs*, 4.
28. **http://airpower.airforce.gov.au/publications/Details/454/157-What-is-Cyberspace-Examining-its-Characteristics.aspx**
29. http://chinadigitaltimes.net/2015/05/china-and-russia-agree-to-respect-cyber-sovereignty/
30. Russia gives Snowden asylum, Obama-Putin summit in doubt http://www.reuters.com/article/us-usa-security-snowden-russia-idUSBRE9700N120130801
31. **US Pentagon to treat cyber-attacks as 'acts of war'**, http://www.bbc.com/news/world-us-canada-13614125
32. Pentagon announces new strategy in cyberwarfare http://www.nytimes.com/2015/04/24/us/politics/pentagon-announces-new-cyberwarfare-strategy.html?_r=0
33. Stewart, P.(2012), “Shamoon Virus Most Destructive Yet for Private Sector, Panetta Says,” Reuters , http://www. reuters.com/article/2012/10/12/us-usa-cyber-pentagon-shimoonidUSBRE89B04Y20121012
34. Principia Cybernetica "Cyberspace" http://pespmc1.vub.ac.be/cybspace.html
35. LaFraniere ,SH. and Ansfield J.(2010), “Cyberspying Fears Help Fuel China’s Drive to Curb Internet,” New York Times, http://query.nytimes.com/gst/fullpage.html?res=9C06E4DF1331F931A25751C0A9669D8B63&pagewanted=all
36. Gorman, S. and Barnes E. J.(2012) “Iran Blamed for Cyber Attacks,” Wall Street Journal, http://www.wsj.com/articles/SB10000872396390444657804578052931555576700
37. Pignal ,S.(2010), “US presses Brussels on terror data swaps,” Financial Times, https://www.ft.com/content/99f8119e-1054-11df-841f-00144feab49a

38. Steve Lohr, "Global Strategy Stabilized IBM During Downturn", New York Times(20 April 2010) http://www.nytimes.com/2010/04/20/technology/20blue.html?_r=0
39. The Economist, "Data, data, everywhere," Special report on managing information, February 27,2010http://www.economist.com/node/15557443
40. managing information, February 27,2010http://www.economist.com/node/15557443
41. The information revolution gets political by JOSEPH S. NYE -THE AUSTRALIAN- FEBRUARY 11, 2013 http://www.theaustralian.com.au/news/world/the-information-revolution-gets-political/story-e6frg6ux-1226574887092
42. Cooper,R. The new liberal imperialism https://www.theguardian.com/world/2002/apr/07/1
43. Nye,J, The velvet hegemon- How soft power can help defeat terrorism http://foreignpolicy.com/2009/11/02/the-velvet-hegemon/
44. Time, 'Enemies at The Firewall', http://www.time.com/time/magazine/article/0,9171,1692063,00.html, 6 December 2007.
45. **U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program** https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html
46. The Pentagon is looking for a few good computer hackers.http://www.usnews.com/news/business/articles/2016-03-02/pentagon-seeking-a-few-good-computer-hackers
47. **Obama Says He Will Name National Cybersecurity Adviser** http://www.washingtonpost.com/wp-dyn/content/article/2009/05/29/AR2009052900350.html
48. Waters, R. and Menn J.(2010), Open Net Initiative , "Closing the frontier," Financial Times ,
49. **Inside the new era of warfare: Exploring the 'cyber arms race' with Mikko Hyppönen**, *By Jason Murdock*, http://www.ibtimes.co.uk/inside-new-era-warfare-exploring-cyber-arms-race-mikko-hypponen-1555084
50. Fackler, M.(2014), "North Korea Accuses U.S. of Staging Internet Failure," New York Times http://www.nytimes.com/2014/12/28/world/asia/north-korea-sony-hacking-the-interview.html
51. Ferguson, N.(2009), "Think Again: Power", Foreign Policy, available at: http://foreignpolicy.com/2009/11/03/think-again-power/

52. Perlroth, N.(2012), “In Cyberattack on Saudi Firm, U.S Sees Iran Firing Back,” New York Times ,http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html
53. Nye, J., & Owens, W. A. (1996). America's information edge. *Foreign affairs*, 20-36.
54. Nye , J. "Get smart: Combining hard and soft power." Foreign Affairs (2009): 160-163
55. Nye, J. (1990). Soft power. *Foreign policy*, (80), 153-171.
56. Nye, J. (2002). Why military power is no longer enough. *The Observer*, *31*, 2002.
57. Nye, J. (2011). The Future of Power, New York. *Public Affairs*, 51.

مواقع حكومية

1. CLINTON, B., & GORE, A. (1996). Excerpts from transcribed remarks by the president and the vice president to the people of Knoxville on internet for schools. *Speech. Knoxville: White House*. http://govinfo.library.unt.edu/npr/library/speeches/101096.html
2. **Britain's cyber security bolstered by world-class strategy"From:HM Treasury, Cabinet Office, The Rt Hon Ben Gummer MP and The Rt Hon Philip Hammond MP,First published:1 November 2016,Part of:Cyber security** https://www.gov.uk/government/news/britains-cyber-security-bolstered-by-world-class-strategy
3. FACT SHEET: President Xi Jinping's State Visit to the United States, https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states
4. Fierce Government IT, ‘Panetta: DoD cyber spending won't be cut’ http://www.fiercegovernmentit.com/story/panetta-dod-cyber-spending-wont-be-cut/2012-01-30, 30 January 2012
5. G20: Growing International Consensus on Stability in Cyberspace,POSTED BY CHRISTOPHER PAINTER,DECEMBER 3, 2011, https://blogs.state.gov/stories/2015/12/03/g20-growing-international-consensus-stability-cyberspace

مواقع الكترونية:

1. http://defense-arab.com/vb/threads/22086/
2. http://en.oxforddictionaries.com
3. http://moodle.oakland.k12.mi.us/os/mod/page/view.php?id=11722

4. http://site.ebrary.com.ezproxy.aub.edu.lb/lib/aub/reader.action?docID=10031906
5. Clinton's Speech on the "Smart Power Approach to Counterterrorism", September 2011Speaker: Hillary Rodham Clinton Published September 9, 2011http://www.cfr.org/counterterrorism/clintons-speech-smart-power-approach-counterterrorism-september-2011/p25854
6. Cyberwar Said To Be The 'New Arms Race' As Nation States Scramble To Boost Capabilities And Defenses http://www.cyberwar.news/2015-10-16-cyberwar-said-to-be-the-new-arms-race-as-nation-states-scramble-to-boost-capabilities-and-defenses.html
7. http://www.internetlivestats.com/total-number-of-websites
8. http://www.internetworldstats.com/pr/edi083.htm
9. http://www.newworldencyclopedia.org/entry/Cyberspace
10. http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/
11. http://www.webopedia.com/TERM/C/cyberspace.html
12. https://blog.dashburst.com/infographic/why-big-data-is-everywhere/ December 5, 2013
13. https://en.wikipedia.org/wiki/Cyberspace
14. **Cyber weapons: 4 defining characteristics** https://gcn.com/Articles/2015/06/04/Cyber-weapon.aspx?Page=1(last visited 19,10,2016)
15. Inside the secret digital arms race: Facing the threat of a global cyberwar **By Steve Ranger** ,http://www.techrepublic.com/article/inside-the-secret-digital-arms-race/
16. Kelly Jackson Higgins, "The Long Shadow of Saudi Aramco," Dark Reading, October 14, 2013, http://www.darkreading.com/attacks-breaches/the-longshadow-of-saudi-aramco/d/d-id/1140664?
17. Key data elements https://www.ibm.com/support/knowledgecenter/SSS28S_3.0.0/com.ibm.help.forms.doc/Authenticated_Clickwrap/i_authclick_g_key_data_elements.html
18. Luiza Ch. Savage, 'Julian Assange: The Man Who Exposed the Downloaded by [King's College London] at 06:51 09 December 2011 Notes| 147World', Macleans, 13 December 2010, http://www2.macleans.ca/2010/12/13/a-man-of-many-secrets/
19. Mike Nathan,**HERF GUN ZAPS MORE THAN YOUR DINNER,** **http://hackaday.com/2011/03/21/herf-gun-zaps-more-than-your-dinner/**

20. **New Report Lifts Curtain On Russia's Construction Of Powerful "Cyberarmy"** https://www.buzzfeed.com/sheerafrenkel/new-report-lifts-curtain-on-russias-construction-of-powerful?utm_term=.spNWyAn7BB#.tawwL58edd
21. Omid Memarian, Internet Yearns to Be Free in Iran, SAN FRANcIScO CHRON., Dec. 9, 2005 http://www.sfgate.com/opinion/openforum/article/International-Human-Rights-Day-Internet-yearns-2590171.php
22. Organization for Economic Co-operation and Development, Glossary of Statistical Terms, Global Commons, http://stats.oecd.org/glossary/detail.asp?ID=1 120 (last visited october. 8, 2016); United Nations Statistics Division, Global Commons Definition, http://unstats.un.orglunsd/environmentgl/gesform.asp?getitem=573
23. Paul Roberts, "Whoddunnit? Conflicting Accounts on Aramco Hack Underscores Difficulty of Attribution," Naked Security, October 30, 2012, http://nakedsecurity.sophos.com/2012/10/30/whodunnit-aramco-hack/
24. **What Are Computer Worms, and How Do They Work? https://www.lifewire.com/how-computer-worms-work-816582**
25. What do computer Virsus do and how to remove and avoid computer viruses? http://miamicomputerrepairsite.com/what-do-computer-viruses-do-how-to-remove-and-avoid-computer-viruses/comment-page-18/
26. What is a Trojan Virus? https://usa.kaspersky.com/internet-security-center/threats/trojans#.WA8N1vl9600
27. **What is Domain Name Resolution** http://www.bleepingcomputer.com/tutorials/what-is-domain-name-resolution/
28. **With 84 million users, Russia's Internet penetration rate has nearly doubled in five years** http://www.ewdn.com/2016/02/08/with-84-million-users-russias-internet-penetration-rate-has-nearly-doubled-in-five-years/
29. **Xi Jinping leads Internet security group** http://webcache.googleusercontent.com/search?q=cache:http://news.xinhuanet.com/english/china/2014-02/27/c_133148273.htm

الفهرست